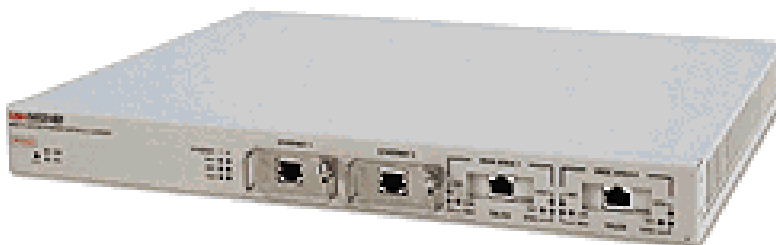


CSX400 AND CSX400-DC USER'S GUIDE



CABLETRON
systems
The Complete Networking Solution™

Notice

Cabletron Systems reserves the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Cabletron Systems to determine whether any such changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL CABLETRON SYSTEMS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF CABLETRON SYSTEMS HAS BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

© Copyright 1997 by Cabletron Systems, Inc., P.O. Box 5005, Rochester, NH 03866-5005

All Rights Reserved

Printed in the United States of America

Part Number: 9032289 September 1997

Cabletron Systems **LANVIEW**, **QuickSET**, and **SPECTRUM** are registered trademarks, and **QuickSTART**, and **CSX400** and **CSX400-DC** are trademarks of Cabletron Systems, Inc.

All other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies.

FCC Notice

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment uses, generates, and can radiate radio frequency energy and if not installed in accordance with the operator's manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference in which case the user will be required to correct the interference at his own expense.

WARNING: Changes or modifications made to this device which are not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

DOC Notice

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la class A prescrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

VCCI Notice

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（V C C I）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Cabletron Systems, Inc. Program License Agreement

IMPORTANT: Before utilizing this product, carefully read this License Agreement.

This document is an agreement between you, the end user, and Cabletron Systems, Inc. (“Cabletron”) that sets forth your rights and obligations with respect to the Cabletron software program (the “Program”) contained in this package. The Program may be contained in firmware, chips or other media. BY UTILIZING THE ENCLOSED PRODUCT, YOU ARE AGREEING TO BECOME BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE AND THE LIMITATION OF WARRANTY AND DISCLAIMER OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY RETURN THE UNUSED PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.

Cabletron Software Program License

1. **LICENSE.** You have the right to use only the one (1) copy of the Program provided in this package subject to the terms and conditions of this License Agreement.

You may not copy, reproduce or transmit any part of the Program except as permitted by the Copyright Act of the United States or as authorized in writing by Cabletron.
2. **OTHER RESTRICTIONS.** You may not reverse engineer, decompile, or disassemble the Program.
3. **APPLICABLE LAW.** This License Agreement shall be interpreted and governed under the laws and in the state and federal courts of New Hampshire. You accept the personal jurisdiction and venue of the New Hampshire courts.

Exclusion of Warranty and Disclaimer of Liability

1. **EXCLUSION OF WARRANTY.** Except as may be specifically provided by Cabletron in writing, Cabletron makes no warranty, expressed or implied, concerning the Program (including its documentation and media).

CABLETRON DISCLAIMS ALL WARRANTIES, OTHER THAN THOSE SUPPLIED TO YOU BY CABLETRON IN WRITING, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE PROGRAM, THE ACCOMPANYING WRITTEN MATERIALS, AND ANY ACCOMPANYING HARDWARE.

2. **NO LIABILITY FOR CONSEQUENTIAL DAMAGES.** IN NO EVENT SHALL CABLETRON OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR RELIANCE DAMAGES, OR OTHER LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THIS CABLETRON PRODUCT, EVEN IF CABLETRON HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, OR ON THE DURATION OR LIMITATION OF IMPLIED WARRANTIES, IN SOME INSTANCES THE ABOVE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU.

United States Government Restricted Rights

The enclosed product (a) was developed solely at private expense; (b) contains “restricted computer software” submitted with restricted rights in accordance with Section 52.227-19 (a) through (d) of the Commercial Computer Software - Restricted Rights Clause and its successors, and (c) in all respects is proprietary data belonging to Cabletron and/or its suppliers.

For Department of Defense units, the product is licensed with “Restricted Rights” as defined in the DoD Supplement to the Federal Acquisition Regulations, Section 52.227-7013 (c) (1) (ii) and its successors, and use, duplication, disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at 252.227-7013. Cabletron Systems, Inc., 35 Industrial Way, Rochester, New Hampshire 03867-0505.

DECLARATION OF CONFORMITY

Application of Council Directive(s): **89/336/EEC**
73/23/EEC
91/263/EEC

Manufacturer’s Name: **Cabletron Systems, Inc.**

Manufacturer’s Address: **35 Industrial Way**
PO Box 5005
Rochester, NH 03867

European Representative Name: **Mr. J. Solari**

European Representative Address: **Cabletron Systems Limited**
Nexus House, Newbury Business Park
London Road, Newbury
Berkshire RG13 2PZ, England

Conformance to Directive(s)/Product Standards: **EC Directive 89/336/EEC**
EC Directive 73/23/EEC
EC Directive 91/263/EEC
EN 55022
EN 50082-1
EN 60950

Equipment Type/Environment: **Networking Equipment, for use in a Commercial or Light Industrial Environment.**

We the undersigned, hereby declare, under our sole responsibility, that the equipment packaged with this notice conforms to the above directives.

Manufacturer	Legal Representative in Europe
<u>Mr. Ronald Fotino</u>	<u>Mr. J. Solari</u>
Full Name	Full Name
<u>Principal Compliance Engineer</u>	<u>Managing Director - E.M.E.A.</u>
Title	Title
<u>Rochester, NH, USA</u>	<u>Newbury, Berkshire, England</u>
Location	Location

Contents

CHAPTER 1 INTRODUCTION

Related Documentation	1
How to Use This Guide	1
Document Conventions.....	3
Getting Help	4

CHAPTER 2 ABOUT THE CSX400

CSX400 Hardware	5
WAN Connection	5
Ethernet LAN Connection	7
Remote Management Capabilities	7
Optional Features	8
CSX400 Firmware Support	8
IEEE 802.3 Ethernet.....	8
WAN Protocols	9
Firmware Data Compression	10
Inverse Multiplexing (IMUX)	10
HDLC	11
DHCP and NAT	11
Point-to-Point Protocol (PPP)	12
PAP and CHAP Security	12
LQM.....	13
Multilink Protocol	13
ISDN	14
ISDN Back-up.....	15
HDSL	16
Bridging and Routing	16
Bridging and Routing Protocol Filtering	18
System Passwords	18
Simple Network Management Protocol (SNMP)	19
Software and Firmware Upgrades	22

CHAPTER 3 ISDN LINE ORDERING AND CONFIGURATION

Arranging ISDN Service	23
Telephone Switch Support	24
ISDN BRI Line Configuration	24
ISDN BRI Configurations	25
SPIDs, Directory Numbers and Telephone Numbers	25
Telephone Switch Parameters	26

CHAPTER 4 PLANNING FOR CSX400 ISDN CONFIGURATION

Configuration Process and Terminology	29
Collect Network Information	30
Names and Passwords	30
ISDN Line Information	31
Network Information Diagrams	32
Network Information Tables	38
Sample Configuration	42
Names and Passwords Example	47

CHAPTER 5 ETHERNET CABLING REQUIREMENTS

Network Requirements	49
10BASE-T Twisted Pair Network	50
Multimode Fiber Optic Network	51
Single Mode Fiber Optic Network	52
10BASE2 Coaxial Cable Network	53
Transceiver Requirements	53

CHAPTER 6 INSTALLATION

Unpacking the CSX400	55
Guidelines for Installations	55
Installing Interface Modules	56
Installing Ethernet Port Interface Modules (EPIMs)	56
Removing the CSX400 Cover	58
Removing the CSX400-DC Cover	59
Installing WAN Port Interface Modules (WPIMs)	60

CSX-COMP/ENCR Installation	62
Installing the CSX400.....	63
Tabletop and Shelf Installations	63
CSX400 and CSX400-DC Rackmount Installation	64
Connecting the CSX400 to the Power Source	68
Connecting the CSX400-DC to the Power Source.....	69

CHAPTER 7 CSX400 CONFIGURATION WITH *QuickSET*

Ethernet Configuration	74
Ethernet 1 and 2 Configuration Window	74
Wide Area 1 and 2 Configuration	79
Wide Area T1 Configuration Window	80
Wide Area E1 Configuration Window	83
Wide Area DI Configuration Window	85
Wide Area Synchronous Configuration Window	88
Wide Area DDS Configuration Window	91
Wide Area HDSL Configuration Window	93
Wide Area Frame Relay Time Slot Configuration Window	95
Wide Area PPP Time Slot Configuration Window	96
Wide Area HDSL Time Slot Configuration Window	98
Bridging and Routing Configuration	99
Bridging and Routing Configuration Window	99
Bridging and Routing (WAN Frame Type) Configuration Window	105
Routing Configuration Window	107
IP Routing Configuration	108
IPX Routing Configuration	108
Advanced Routing Configuration Window	111
QuickSET Pull-Down Menus.....	117
File Menu	117
Firmware Upgrade Menu	119
Advanced Configuration Menu	122
Compression and Congestion Window	123

CHAPTER 8 GENERAL CONFIGURATION USING LOCAL MANAGEMENT

Chapter Organization	125
Local Management Overview.....	126
Management Agent	126
Local vs. Remote Management.....	126
Local Management Screen Elements.....	127
Local Management Keyboard Conventions.....	129
Navigating Within Local Management Screens.....	130
Establishing a TELNET Connection	131
Local Management Screen Hierarchy	131
Accessing Local Management	132
Using the Menu Screens	132
Main Menu Screen	133
Setup Menu Screen	134
System Level Screen	135
Setting the System Date	138
Setting the System Time	138
Setting the Host IP Address	139
Setting the Subnet Mask	139
Setting the Default Gateway	139
Setting the Default Interface	140
SNMP Community Names Screen.....	141
Community Name Access Policy.....	141
Setting SNMP Community Names	142
SNMP Traps Screen	143
Trap Table Screen Fields	143
Setting the SNMP Trap Destination.....	144
Flash Download Screen	145
Selecting a Flash Download Method	146

Bridge Setup Screen	149
Bridge Setup Screen Fields	149
Selecting a Spanning Tree Protocol	150
Selecting the Bridge Port Administrative Status	150
Selecting the Bridge Port Pair Administrative Status	151
Router Setup Screen	152
Router Setup Fields	152
IP Configuration Screen	153
IP Configuration Screen Fields	153
IP General Config Screen	154
IP General Configuration Status Fields	154
IP General Configuration Fields	155
Enabling the RIP Routing Protocol on a Port	160
IPX Configuration Screen	162
IPX Configuration Fields	162
IPX General Configuration Screen	163
IPX General Configuration Status Fields	163
IPX General Configuration Fields	164
IPX Routing over Frame Relay	167
Enabling the IPX SAP Routing Protocol on a Port	168
Enabling RIP on a Port	170
WAN Setup	172
WAN Physical Configuration Screen Fields	173
WAN Interface Configuration Screen	174
WAN Interface Configuration Screen Fields	174

CHAPTER 9 MIB NAVIGATOR

Chapter Organization	177
MIB Navigator Screen	178
Managing Device MIBs	178
MIB Navigator Command Set Overview	179
Conventions for MIB Navigator Commands	180
Navigation Commands	181
Other Commands	190
Special Commands	203

CHAPTER 10 TROUBLESHOOTING

Troubleshooting CSX400 Hardware	208
Power (PWR) LED is OFF	208
Processor (CPU) LED is OFF	208
Processor (CPU) LED is RED	208
Troubleshooting the LAN	208
Collision (CLN) LED is RED	208
Link (LNK) LED is OFF	208
Troubleshooting the WAN	209
Link (LNK) LED is OFF	209
Link (LNK) LED is RED	209
Link (LNK) LED is AMBER	209
Status 1 (STS1) LED is OFF	209
Status 1 (STS1) LED is RED	210
Status 1 (STS1) LED is AMBER	211
Status 1 (STS1) LED is GREEN	211
Status 2 (STS2) LED is OFF	212
Status 2 (STS 2) LED is RED WPIM-HDSL Installed in CSX400	213
Status 2 (STS2) LED is AMBER	213
Status 2 (STS2) LED is GREEN	213
Test (TST) LED is AMBER (blinking)	214
Investigating Software Configuration Problems	214
Connection to Device Fails During Software Configuration	214
User Cannot Communicate with Remote Network Station	215

APPENDIX A EPIM SPECIFICATIONS

Introduction	217
EPIM-T	217
EPIM-F1 and EPIM-F2	218
EPIM-F3	220
EPIM-C	221
Connector Type	221
Grounding	221
EPIM-A and EPIM-X (AUI Port)	222

APPENDIX B WPIM CABLE SPECIFICATIONS

WPIM-T1 223

WPIM-SY 225

 EIA-449..... 226

 V.35 227

 EIA-232..... 229

 X.21 230

 EIA-530, EIA-530 ALT A, EIA-530 A, and EIA-530 A ALT A..... 231

WPIM-DDS..... 233

WPIM-E1 234

WPIM-DI..... 236

WPIM-HDSL..... 237

WPIM-S/T..... 238

APPENDIX C SPECIFICATIONS AND STANDARDS COMPLIANCE

CSX400, CSX400-DC, and WPIM Environmental Requirements..... 239

CSX400 Specifications and Compliance Standards 239

CSX400-DC Specifications and Compliance Standards..... 240

CSX400 and CSX400-DC Regulatory Compliance..... 240

CSX400-DC Regulatory Compliance (Only) 240

Individual WPIM Regulatory Compliance..... 241

 WPIM-TI 241

 WPIM-SY 242

 WPIM-DDS 242

 WPIM-E1 243

 WPIM-DI 243

 WPIM-S/T 243

 WPIM-HDSL 244

APPENDIX D NETWORK INFORMATION WORKSHEETS

APPENDIX E FCC PART 68 - USER’S INFORMATION FOR CSX400 AND CSX400-DC

APPENDIX F GLOSSARY

INDEX

1

Introduction

Welcome to the Cabletron Systems **CSX400 and CSX400-DC User's Guide**. This guide provides basic configuration information, hardware specifications and troubleshooting tips for the CSX400 and CSX400-DC. This guide also provides background information about 10BASE-T Ethernet Local Area Networks (LANs) and guidelines for routing and bridging over Wide Area Networks (WANs).



The CSX400 and CSX400-DC have identical features and functions with the exception of their power source connection. The CSX400 connects to an ac power source and the CSX400-DC connects to a dc power source. Both the CSX400 and the CSX400-DC are referred to as the CSX400, unless otherwise specified in this guide.

Related Documentation

Use the ***READ ME FIRST!*** document included with the CSX400 to set up your computer before starting configuration.

Use the Cabletron Systems ***QuickSTART Guide*** (the CD insert of the *QuickSET* CD case) to install the CSX400.

Use the appropriate Cabletron Systems WPIM Local Management Guide to connect your CSX400 to a WAN using a TELNET connection.

How to Use This Guide

This guide along with the ***READ ME FIRST!*** document and the ***QuickSTART Guide*** provide the necessary information to install and configure the CSX400. Read all of these documents before installing the CSX400.

This guide is organized as follows:

Chapter 1, Introduction, details document conventions and provides information on getting help.

Chapter 2, About the CSX400, describes the hardware components and software protocols and features.

Chapter 3, ISDN Line Ordering and Configuration, provides the information you need to order ISDN service from the telephone company.

Chapter 4, Planning for CSX400 ISDN Configuration, describes the router configuration process.

Chapter 5, Ethernet Cabling Requirements, describes the basic cabling requirements for an Ethernet Local Area Network (LAN).

Chapter 6, Installation, provides detailed installation instructions for attaching the CSX400 and CSX400-DC to a network.

Chapter 7, CSX400 Configuration with QuickSET, provides instructions on connecting the CSX400 to a Wide Area Network (WAN) using Cabletron Systems *QuickSET* management utility.

Chapter 8, General Configuration Using Local Management, provides instructions for configuring the CSX400 through a TELNET connection.

Chapter 9, MIB Navigator, explains how to use the MIB Navigator utility.

Chapter 10, Troubleshooting, provides detailed troubleshooting tips using the LANVIEW LEDs on the CSX400.

Appendix A, EPIM Specifications, provides hardware specifications and pinout information for available Cabletron Systems Ethernet Port Interface Modules (EPIMs).

Appendix B, WPIM Cable Specifications, provides part number and connector information for WPIMs.

Appendix C, Specifications and Standards Compliance, contains hardware specifications and safety and compliance standards for the CSX400.

Appendix D, Network Information Worksheets, provides blank network information worksheets.

Appendix E, FCC Part 68 - User's Information For CSX400 and CSX400-DC, provides instructions required to comply with FCC Rules, Part 68.

Appendix F, Glossary, defines commonly used terms.

Document Conventions

The following conventions are used throughout this guide:



Note symbol. Calls the reader's attention to any item of information that may be of special importance.



Tip symbol. Conveys helpful hints concerning procedures or actions.



Caution symbol. Contains information essential to avoid damage to the equipment.



Electrical Hazard Warning symbol. Warns against an action that could result in personal injury or death due to an electrical hazard.



Warning symbol. Warns against an action that could result in personal injury or death.

Getting Help

If you need additional support related to this device, or if you have any questions, comments, or suggestions concerning this manual, contact the Cabletron Systems Global Call Center:

Phone	(603) 332-9400
Internet mail	support@ctron.com
FTP Login Password	ctron.com (134.141.197.25) <i>anonymous</i> <i>your email address</i>
BBS Modem setting	(603) 335-3358 8N1: 8 data bits, No parity, 1 stop bit
For additional information about Cabletron Systems or our products, visit our World Wide Web site: http://www.cabletron.com/ For technical support, select Service and Support .	

Before calling the Cabletron Systems Global Call Center, have the following information ready:

- Your Cabletron Systems service contract number
- A description of the failure
- A description of any action(s) already taken to resolve the problem (e.g., changing mode switches, rebooting the unit, etc.)
- The serial and revision numbers of all involved Cabletron Systems products in the network
- A description of your network environment (layout, cable type, etc.)
- Network load and frame size at the time of trouble (if known)
- The device history (i.e., have you returned the device before, is this a recurring problem, etc.)
- Any previous Return Material Authorization (RMA) numbers

2 About the CSX400

The CSX400 (**Figure 1**) is an access device that provides Ethernet Local Area Network (LAN) connectivity via two Ethernet Port Interface Modules (EPIMs), and offers high-speed Wide Area Network (WAN) access to remote sites via two WAN Port Interface Modules (WPIMs). The CSX400 supports IEEE 802.1d transparent bridging, IP and IPX routing, ISDN, Dynamic Host Configuration Protocol (DHCP), Network Address Translation (NAT) routing, and Inverse Multiplexing (IMUX) between Ethernet LANs across a WAN.

The CSX400 operates from a standard ac power source and the CSX400-DC operates from a dc voltage source to meet all the requirements for installation into Telephone Central Office facilities.

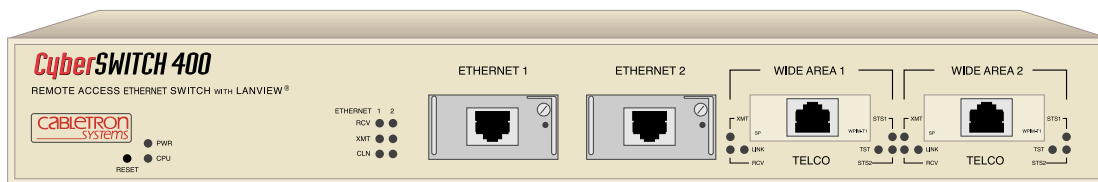


Figure 1 The CSX400

CSX400 Hardware

This section details the CSX400 hardware capabilities.

WAN Connection

The CSX400 supports Point-to-Point Protocol (PPP) including: Link Control Protocol (LCP), BNCP, IPCP, IPXCP, LQM, Multilink Protocol (MP) and CHAP and PAP, ISDN-BRI and Frame Relay protocols through one of the following WAN port interface modules (WPIMs):

- The WPIM-T1 provides a T1 interface through a front panel RJ45 port and includes a built-in Channel Service Unit/Digital Service Unit (CSU/DSU) for direct connection to a T1 line. The WPIM-T1 provides both Full T1 or Fractional T1 using 56 or 64 Kbps Time Slots, with a total throughput of up to 1.544 Mbps.

- The WPIM-Sync provides a synchronous serial connection of up to 2.048 Mbps to external communications equipment (e.g., a multiplexer or CSU/DSU). The WPIM-Sync uses a subminiature 26-pin connector that supports the electrical signal interfaces listed below. **Appendix B**, provides complete part number and cable pinout information for the following electrical signal interfaces:
 - EIA-RS449
 - V.35
 - EIA-RS232D
 - X.21
 - EIA-RS530
 - EIA-530A
 - RS530 ALT A
 - RS530A ALT A
- The WPIM-DDS provides a 56 Kbps or 64 Kbps Digital Data Service (DDS) connection. The WPIM-DDS supports remote CSU diagnostic or 64 Kbps clear channel loopback and non-latching remote DSU diagnostic loopback.
- The WPIM-E1 provides an E1 interface through a front panel RJ45 port and includes a built-in CSU/DSU for direct connection to an E1 line. The WPIM-E1 provides both Full E1 or Fractional E1 using 56 or 64 Kbps Time Slots with a total throughput of up to 2 Mbps.
- The WPIM-DI provides a T1 interface through a front panel RJ45 port and includes a built-in CSU/DSU for direct connection to a T1 line. The WPIM-DI provides both Full T1 or Fractional T1 using 56 or 64 Kbps Time Slots and also provides a second Drop-and-Insert interface, which allows more than one device, such as a PBX, to share a single T1 connection.
- The WPIM-S/T provides an Integrated Services Digital Network (ISDN) 128 Kbps Basic Rate Interface (BRI) for the CSX400. The WPIM-S/T provides an ISDN back-up link for a remote site or branch office when the main WPIM for a frame relay or leased line loses a connection or becomes disabled. An NT-1 adapter is necessary for this interface in the United States.
- The WPIM-HDSL provides a connection for users in a campus environment, or have access to local subscriber loops, who want to send their data over their existing telephone lines, that may run between floors, buildings, or other physical structures, at rates of up to 1.544Mbps. HDSL supports line lengths of up to 3, 657 meters (12,000 feet) over 24 American Wire Gauge (AWG) Unshielded Twisted Pair (UTP) cabling.

- The WPIM-T1/DDS provides both a T1 and DDS interface that allows you to easily switch between the two interfaces by changing the physical cabling and reconfiguring QuickSET for the desired interface. The WPIM-T1/DDS has the capabilities of both the WPIM-T1 and WPIM-DDS.

Ethernet LAN Connection

The CSX400 provides 10 Mbps Ethernet/IEEE 802.3 support through two Cabletron Systems Ethernet Port Interface Modules (EPIMs), which are available in a variety of media types.

Appendix A, EPIM Specifications, details the available EPIMs that can be used to configure the CSX400 for an Ethernet connection.

FLASH EEPROMs — The CSX400 uses a FLASH Electrically Erasable Programmable Read-Only Memory (EEPROM) that allows new and updated firmware to be downloaded in conjunction with Cabletron Systems *QuickSET* or any device using BootP or TFTP protocols.

LANVIEW LEDs — Cabletron Systems LANVIEW Status Monitoring and Diagnostics System is a troubleshooting tool that helps in the diagnosing of power failures, collisions, cable faults, and link problems. The LANVIEW LEDs are located on the CSX400 front panel.

RESET Button — The front panel RESET button reboots the CSX400 and initializes the processor. The RESET button also is used with the mode switches to clear NVRAM.

Remote Management Capabilities

The CSX400 can be remotely managed with any SNMP network management system including the following:

- Cabletron Systems SPECTRUM for Open Systems
- Cabletron Systems Remote SPECTRUM Portable Management Applications (SPMAs)
- Cabletron Systems *QuickSET*
- Cabletron Systems SPECTRUM Element Manager (SPEL)
- Third Party SNMP compliant Network Management Packages

Optional Features

Rack Mounting Capabilities — The CSX400 can be installed in a 19-inch rack with the included mounting brackets and screws. Refer to **Chapter 6 Installation**, for complete rack mounting instructions.

Hardware Data Compression Module (CSX-COMP/ENCR) — The same industry standard STAC Electronics Stacker LZS Compression algorithm supported by CSX400 software is made available by an optional hardware data compression module that accelerates data compression for the CSX400 over PPP and Frame Relay. Depending on the packet type and size, hardware data compression provides a minimum of 2:1 data compression, giving 3 Mbps throughput on each T-1 WPIM interface. To use the hardware data compression module, compatible equipment (such as the CSX400, CSX200, and HSI-M-W6 or other vendors' equipment which conforms to the applicable standards), must be in use at both ends of the WAN link. When the hardware data compression module is installed on the board, it automatically assumes the compression task from software. There is no configuration necessary to prioritize hardware over software compression.

CSX400 Firmware Support

The CSX400 firmware supports IEEE 802.1d bridging, and IP and IPX routing, and OSI Layer 2 Inverse Multiplexing (IMUX), which allows both WAN channels to be used as a single, high bandwidth, WAN channel. Wide Area Networking includes **Point-to-Point Protocol (PPP)**, **Frame Relay**, and ISDN. Remote access is via Full or Fractional T1, E1, Synchronous, Digital Data Service, ISDN BRI, or HDSL connections.

This device supports industry-standard protocols, security features, compression algorithms and network management tools to ensure interoperability with equipment from other vendors.

IEEE 802.3 Ethernet

The CSX400 provides a standard 802.3 Media Access Control (MAC) layer for Ethernet communications. All bridging and routing protocols are supported across the Ethernet link.

WAN Protocols

This device supports the following WAN protocols over the WAN port:

- Point-to-Point Compression Control Protocol (CCP) as defined by RFC 1962
- Inverse Multiplexing (IMUX)
- Dynamic Host Configuration Protocol (DHCP) as defined by RFC 1541
- Network Address Translation (NAT) routing as defined by RFC 1631
- Point-to-Point Protocol (LCP) as defined by RFC 1661
- Point-to-Point Protocol (BNCP) as defined by RFC 1638
- Point-to-Point Protocol (IPCP) as defined by RFC 1332
- Point-to-Point Protocol (IPXCP) as defined by RFC 1552
- Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) under PPP as defined by RFC 1994
- Point-to-Point Protocol Line Quality Monitoring (LQM) as defined by RFC 1333
- Point-to-Point Protocol Multilink Protocol (MP) as defined by RFC 1717
- Integrated Services Digital Network (ISDN) Basic Rate Interface (BRI) as defined by Q.921/Q.931
- Frame Relay Link Management Interface (LMI) as defined by ANSI T1.617 Annex D and ITU Q.933 Annex A
- Frame Relay Data Encapsulation as defined by RFC 1490
- Frame Relay Data Compression Protocol (DCP) as defined by FRF.9

PPP is a data link layer industry standard WAN protocol for transferring multi-protocol data traffic over point-to-point connections. With this protocol, options such as security data compression, and network protocols can be negotiated over the connection.

Frame Relay is a packet-switching data communications protocol that statistically multiplexes many data conversations over a single transmission link. Data compression allows Frame Relay to negotiate compression over Frame Relay permanent virtual channels (PVCs).

ISDN BRI is a switched Data Link layer control protocol which uses digital signaling to place a call into an ISDN network. Once the call is made, PPP is then used to transfer data.

Firmware Data Compression

The STAC Electronics Stacker LZS Compression algorithm provides a minimum of 2:1 firmware data compression for the CSX400 over PPP and Frame Relay. Firmware data compression is supported in software on each WAN interface for line speeds of up to 256 Kbps. per WPIM, which is equivalent to four DS0 channels. To use data compression, compatible equipment, (such as the CSX400, CSX200, and HSIM-W6 or other vendors' equipment which conforms to the applicable standards), must be in use at both ends of the WAN link. This firmware method of data compression is used as the default, if the hardware compression module is not installed.

Inverse Multiplexing (IMUX)



Cabletron Systems products that support IMUX, such as the CSX400, HSIM-W6 and HSIM-4T1, must exist on both ends of the WAN link for the IMUX function to work.

Both bridging and routing functions are disabled when using the IMUX function.

Cabletron Systems Inverse Multiplexing (IMUX) feature provides enhanced throughput for users by doing each of the following:

- The IMUX function evenly distributes a data packet stream from the LAN interface through the two WAN interfaces on the CSX400. Since the data traffic is equally shared between the two Full T1 interfaces, each with 1.5 Mbps throughput, the total throughput over the logical link is 3 Mbps, or 6 Mbps full-duplex operation with the optional hardware compression module (CSX-COMP/ENCR) installed in the CSX400.
- The IMUX function passes packet sequence information over the WAN using the Point-to Point Protocol (PPP) and a WAN Encapsulated Ethernet Frame Type to support data coherency on both ends of the link.
- Data packet streams received by the WAN Interfaces on the CSX400 at the other end of the WAN link are then recombined, ordered, and transmitted to the Ethernet 1 interface.
- The IMUX function is fully configurable using *QuickSET*, which is discussed in the **Bridging and Routing Configuration** section of **Chapter 7** and the MIB Navigator command set in **Chapter 9**.

HDLC

Cabletron Systems has provided the High-level Data Link Control (HDLC) protocol which is used in conjunction with the Inverse Multiplexing (IMUX) feature and the WPIM-HDSL to conserve a user's WAN bandwidth between two Cabletron Systems products, over a point-to-point connection. Cabletron Systems products such as the CSX400, CSX200, and HSIM-W6 must be in use on both ends of the WAN link for these functions to work. The HDLC (RAW) protocol reduces the amount of overhead information that needs to be contained within each data packet to direct it to its destination. This decreased packet overhead provides the IMUX and HDSL functions with more bandwidth to transfer user data.

DHCP and NAT

The Dynamic Host Configuration Protocol (DHCP) and Network Address Translation (NAT) method eliminates the expense of purchasing limited public IP addresses for each client on a local network, and the need to re-configure a client if it is moved to a different network.

The CSX400 acts as a DHCP server that allows individual clients (PCs, network equipment) to take turns using a range of private IP addresses (often referred to as local IP addresses), and provides optional secondary setup features for these clients on a per-port basis. The CSX400 distributes these addresses dynamically assigning a local IP address to an individual client from a range of 253 available addresses in its table on a first-come-first-served basis. This local IP address is then "leased" for a predetermined amount of time, which is configured for the particular port. Each Ethernet port provides DHCP services for one Class C subnet and secondary setup features for individual clients that support the use of a default gateway, domain name and WINs server.

On the Wide Area Network (WAN) side, the Network Address Translation (NAT) routing method is used to enable clients assigned with local IP addresses to use the public IP address(es) of the CSX400 WAN interface(s) to access the WAN.



A private or "local" network is referred to as a sub network that is using private or "local" IP addresses. An "outside" network refers to a Wide Area Network (WAN) commonly known as an Internet, an intranet is an "Internet" in use on a facility or campus where registered public IP addresses are required.

The NAT method allows several DHCP clients on a sub network to connect to WAN clients by allowing the DHCP clients to share a single public IP address. When the CSX400 uses NAT, the NAT method modifies the IP headers and addresses, and the selected fields in upper layer protocol headers. This is done to replace the hidden local IP addresses from the sub network with one or more public InterNic assigned IP addresses that can be sent over the outside network on the CSX400 WAN interfaces. Once the CSX400 is assigned at least one public IP address, over 250 IP clients can share this address simultaneously using NAT. This public IP address is assigned statically by the Internet Service Provider (ISP).

Point-to-Point Protocol (PPP)

PPP is a data link layer industry standard WAN protocol for transferring multi-protocol data traffic over point-to-point connections. It is suitable for both high-speed synchronous ports as well as lower speed asynchronous dial-up ports. With this protocol, options such as security and network protocols can be negotiated over the connection.

This device supports synchronous PPP over the ISDN port. In Single Link Mode, PPP uses one ISDN B channel for data transmission. PPP runs over each ISDN B channel for two separate conversations (split B-channel). In Multi-Link Protocol Mode, PPP simultaneously sends and receives data over two ISDN B-channels on the same connection to optimize bandwidth usage.

The STAC Electronics Stacker LZS Compression Protocol is supported over PPP providing up to 4:1 data compression.

PAP and CHAP Security

The CSX400 supports the Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) under PPP.

PAP provides verification of passwords between devices using a 2-way handshake. One device (peer) sends the system name and password to the other device (authenticator). Then the authenticator checks the peer's password against the configured remote peer's password and returns acknowledgment.

CHAP is more secure than PAP as unencrypted passwords are not sent across the network. CHAP uses a 3-way handshake and supports full or half-duplex operation.

In half-duplex operation, the authenticator device challenges the peer device by generating a CHAP challenge, and the challenge contains an MD5 algorithm with a random number that has your encrypted password and system name. The peer device then applies a one-way hash algorithm to the random number and returns this encrypted information along with the system name in the CHAP response. The authenticator then runs the same algorithm and compares the result with the expected value. This authentication method depends upon a password or secret, known only to both ends locally.

Full-duplex operation places an additional step to the half-duplex operation that mirrors the operation discussed above for a peer to validate the authenticator. The peer device challenges the authenticator by generating a CHAP challenge, and the authenticator returns a CHAP response.

The peer device challenges the authenticator device by generating a CHAP challenge, and the challenge contains an MD5 algorithm with a random number that has your encrypted password and system name. The authenticator device then applies a one-way hash algorithm to the random number and returns this encrypted information along with the system name in the CHAP response. The peer device then runs the same algorithm and compares the result with the expected value. This authentication method depends upon a password or secret, known only to both ends locally.

LQM

Link Quality Monitoring (LQM) is a link control mechanism used with PPP to determine when and how often a link is dropping data in units of packets and octets. Link Quality Monitoring accomplishes this by providing Link-Quality-Reports to determine if the quality of the link is adequate for operation. Link Quality Monitoring provides separate measurements for both incoming and outgoing packets that are communicated to both ends of the link. The PPP LQM mechanism carefully defines the Link-Quality-Report packet formats, and specifies reference points for all data transmission and reception measurements. The LQM implementation maintains successfully received packet and octet counts, and periodically transmits this information to its peer using Link-Quality-Report packets.

Multilink Protocol

Multilink Protocol (MP) is an extension of PPP that controls the way frames are transferred across several links whenever a single link is not sufficient to meet the requirements of your present traffic load. Multilink Protocol establishes several simultaneous links between two end points over switched circuits (dial-up lines) in an ISDN network, and dynamically adjusts the bandwidth demands between available links to maintain an effective data transfer.

ISDN

ISDN provides an inexpensive switched digital access to remote sites. The ISDN BRI standard provides for two high speed 64 Kbps bearer (B) channels used for voice or data connections and one 16 Kbps signaling data (D) channel used for call setup, signaling and other information. ISDN allows all types of information to be transmitted including voice, data, fax and video. Multiple devices can be linked to a single ISDN connection, each having their own telephone number. Two or more channels can be combined into a single larger transmission pipe offering variable transmission speeds.

The CSX400 supports one ISDN BRI line and either or both of the B channels for transferring data. If the two B channels are used for separate connections, each provides up to 64 Kbps transfer rates. Both channels can be used together to provide uncompressed data transfer at up to 128 Kbps. The CSX400 can also transfer compressed data at up to 512 Kbps.

A Network Terminator device (NT1) provides the interface between ISDN terminal (router) equipment and the ISDN service provider. In the U.S., the NT1 is provided by the customer; outside the U.S., the NT1 is provided by the ISDN service provider. The CSX400 supports the WPIM-S/T by providing an S/T interface that requires an external NT1.

Telephone Switch Support

The following telephone switch types are supported within the U.S.:

- **National ISDN 1 (NI-1)**
- **AT&T 5ESS with Custom Software**
- **DMS-100**

Outside of the U.S. the following switch types are supported:

- NET3 (European ISDN)
- NET3SW (European Swiss-variant)
- NTT (Nippon Telegraph and Telephone)
- KDD (Kokusai Denshin Denwa Co., Ltd.)
- French Delta (VN4) switches

ISDN Back-up

The ISDN back-up feature provides a back-up link for a remote site or branch office when one or more primary WAN interfaces for a frame relay circuit or a nailed-up PPP connection fails. The WPIM-S/T serves as the backup medium for this primary connection. The WPIM-S/T uses the ISDN interfaces to back-up any primary interfaces which have been configured for ISDN back-up.

Time to Connect, Time to Disconnect, Connect Retries, Back-up Override, Input Idle Time-out and Output Idle Time-out, are the six back-up parameters used to manage the ISDN Back-up feature on the CSX400, and are described as follows:

Time to Connect — Time to Connect allows you to configure the amount of seconds the primary interface can be in a failed state, before attempting to switch over to the back-up interface.

Time to Disconnect — Time to Disconnect allows you to configure the amount of seconds the restored primary interface must remain connected, before attempting to switch over from the back-up interface.

Connect Retries — Connect Retries allows you to configure the number of tries to restore the back-up interface, before giving up.

Backup Override — Backup Override forces the back-up interface to remain connected, and does not allow the back-up interface to switch back to the primary interface, even if the primary interface is restored.

Input Idle Time-out — Input Idle Time-out allows you to determine the amount of time necessary for data packets to be received, before the interface is automatically disconnected.

Output Idle Time-out — Output Idle Time-out allows you to determine the amount of time necessary for data packets to be transmitted, before the interface is automatically disconnected.

HDSL

High-bit rate Digital Subscriber Line (HDSL) technology uses existing copper twisted pair cables designed for conventional analog voice transmission from a telephone carrier servicing area as a low-cost alternative to the quality and speed of fiber optic cables, and provides high-speed full-duplex digital transmission links of up to 1.544 Mbps. The WPIM-HDSL is easy to install in your network over existing telephone lines, and it is a portable investment if a business, or individual user plans to relocate.

HDSL is a direct connection technology that allows connections to be made for distances of up to 12,000 feet over 24 American Wire Gauge (AWG) unconditioned Twisted Pair wire. To obtain the Full T1 line Rate of 1.544 Mbps, two wire pairs are necessary (four wires). If one pair of wires is used (two wires), then data rates of 772 Kbps are supported, which is equivalent to one-half of a T1 line.

Bridging and Routing

Bridging — Bridging connects two or more separate networks together. The bridge examines a portion of each network frame called the header. This header contains control information for the frame. The bridge compares the destination address of the frame to a table of source addresses (bridges dynamically learn the physical location of devices by logging the source addresses of each frame and the bridge port the frame was received on in the source address table). In transparent bridging, the decision to forward the frame is based on this comparison. If the address indicates that the sending station and the destination station are on the same side of the bridge, the frame is not forwarded across the bridge. If the addresses do not indicate that, the bridge forwards the broadcast frame across the bridge to the other network(s).

Bridging allows frames to be sent to all destinations regardless of the network protocols used. It also allows protocols that cannot be routed (such as NETBIOS) to be forwarded, and optimizes internetwork capacity by localizing traffic on LAN segments. A bridge extends the physical reach of networks beyond the limits of each LAN segment. Filters can be used to increase network security in bridged networks, and restrict message forwarding by using user-built address tables (non-transparent bridging).

Routing — Routing provides a way to transfer user data from source to destination over different LAN and WAN links using one or more network protocol formats. Routing relies on routing address tables to determine the best path for each packet. Routing tables can be seeded (i.e., addresses for remote destinations are placed in the table along with network address masks and a metric for path latency). Routing tables are also built dynamically (i.e., the location of remote stations, hosts and networks are updated through inter-router protocols). Routing helps to increase network capacity by localizing traffic on LAN segments and broadcasts that would result from bridged traffic. It also provides security by isolating traffic on segmented LANs. Routing extends the world-wide reach of networks.

CSX400 Bridging and Routing — The CSX400 can operate as a bridge, a router, or both. The CSX400 operates as a router for network protocols that are supported when routing is enabled and operates as a bridge when bridging is enabled. When both bridging and routing are enabled, routing takes precedence over bridging; i.e., the CSX400 uses the protocol address information of the packet to route the packet to the correct destination. However, if the protocol is not supported, the CSX400 operates as a bridge and uses the MAC address information to send the packet.

Operation of the CSX400 is influenced by routing and bridging controls and filters set during CSX400 configuration. General IP routing, and routing or bridging from specific remote routers are controls set during the configuration process.

IEEE 802.1d Bridging — The CSX400 supports the IEEE 802.1d standard for LAN to LAN bridging. Bridging is provided over PPP and Frame Relay as well as adjacent LAN ports. The bridging software uses transparent bridging. When the CSX400 is configured as a bridge, the unit bridges data packets to the destination, regardless of the network protocols used.

The CSX400 uses the Spanning Tree Algorithm to provide bridging redundancy while preventing data loops and duplicate data. This is a self-learning bridge, i.e., the bridge builds and updates an address table with each MAC source address and associated information when the packets are received.

IP Routing — IP routing support provides the ability to process **TCP/IP** frames at the network layer for routing. IP routing support includes the Routing Information Protocol (RIP) that allows the exchange of routing information on a TCP/IP network. The CSX400 receives and broadcasts RIP messages to adjacent routers and workstations.

IPX Routing — Internet Packet Exchange (IPX) routing support provides the ability to process Novell proprietary frames at the network layer for routing. IPX routing support includes both Routing Information Protocol (RIP) and Service Advertising Protocol (SAP) that allows the exchange of routing information on a Novell NetWare network. The SAP provides routers and servers containing SAP agents with a means of exchanging internetwork service information.

Bridging and Routing Protocol Filtering

Filtering is used to allow efficient usage of network resources and provide security for your network and hosts.

IP Internet Firewall — The CSX400 supports IP Internet Firewall filtering to prevent unauthorized access to your system and network resources from the Internet or a corporate Intranet. Security can be configured to permit or deny IP traffic. The security is established by configuring IP access filters, which are based on source IP address, source mask, destination IP address, destination mask, protocol type, and application port identifiers for both Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) protocols. These IP access filters allow individual IP source and destination pair filtering as well as IP address ranges and wild carding to match any IP address. These Firewall filters can be defined to allow inbound only, outbound only, or bi-directional IP communication up to the UDP and TCP application port level. Firewall access filters provide a lot of flexibility to establish a powerful IP security barrier. The CSX400 supports the IP Access Control (from the ctip-mib) Internet Firewall Filter.

Bridge Filtering — Bridge filtering allows a network administrator to control the flow of packets across the CSX400. Bridge filtering can be used to “deny” or “allow” packets based on a “matched pattern” using a specified position and hexadecimal content within the packet. This enables restricting or forwarding of messages based on address, protocol, or data content. Common uses include preventing access to remote networks, controlling unauthorized access to the local network, and limiting unnecessary traffic.

The CSX400 supports the following Bridge Filters:

- dot1dStatic Filters (IETF RFC1493)
- Ethernet Special Filtering Database (from the ctbridge-mib)

System Passwords

System passwords allow you to control access to the CSX400 by establishing three passwords. Each password provides varying levels of access to the CSX400. The default password for each access level is pre-set to *public*. If you do not wish to establish a password, press ENTER, the default password is automatically selected.

The following definitions explain each of the three levels of access:

read-only — This access level allows reading of device parameters not including system passwords.

read-write — This access level allows editing of some device configuration parameters not including changing system passwords.

super-user — This access level allows full management privileges. At this level you must access the CSX400 to run *QuickSET*.

Simple Network Management Protocol (SNMP)

The CSX400 provides SNMP agent support for the following: standard and Enterprise Specific Management Information Bases (MIBs), and support for standard and Enterprise Specific SNMP Traps. SNMP is also used internally for configuration of the CSX400. The active SNMP agent within the CSX400 accepts SNMP requests for status, statistics and configuration updates. Communication with the SNMP agent occurs over the LAN or WAN connection. Any management application using SNMP over **UDP/IP** has access to the local SNMP agent.

SNMP MIB Support

SNMP MIBs are databases of objects used for managing and determining the status and configuration of an SNMP compliant device.

The following SNMP MIBs are supported by the CSX400:

- MIB IIRFC1213
- RMON MIBRFC1271
- DS1 and E1 MIBRFC1406(Digital Signal Level 1 [T1/E1 interface types])
- IETF Bridge MIBRFC1493
- IP Forwarding MIB RFC1354
- PPP LCP MIBRFC1471(Point-to-Point Protocol, Link Control Protocol)
- PPP IPCP MIBRFC1473(IP Control Protocol)
- PPP BNCP MIBRFC1474(Bridge Network Control Protocol)
- IPXCP MIBRFC1552
- Frame Relay DTE MIBRFC1490
- Security MIBRFC1472(CCP, PAP, and CHAP)
- RS-232 MIBRFC1317
- LQM MIBRFC1989
- PPP MP MIBRFC1990

Cabletron Enterprise MIBs

Cabletron Enterprise MIBs include the following: CTWAN-MIB, CTMIB2-EXT-MIB, CTDOWNLOAD-MIB, CTBRIDGE-MIB, RREV-4-MIB, CTROUTER-MIB, CTFAULT-MIB, CTIP-MIB, CHASSIS-MIB, CTNETDIAG-MIB, IP-MIB, IPX-MIB, CTDEFAULT-MIB, CTNAT-MIB.TXT, CTDHCP-MIB.TXT, CTWAN-IMUX-MIB, CTISDN-DIALCONTROL-MIB, CTISDN-DCHANNEL-MIB, and CTISDN-REMOTEPROFILE-MIB.

SNMP Trap Support

SNMP Traps are notifications of network events sent by an SNMP compliant device to an SNMP management station.

The following SNMP Traps are supported by the CSX400:

IETF Standard Traps:

- Warm Start Trap Type Code #1RFC1214
- Bridge New Root TrapType Code #1RFC1493
- Bridge Topology Change TrapType Code #2RFC1493

Cabletron Enterprise Traps:

- Port Segmented TrapType Code #257(0x101)rrev4-mib
- Port Operational TrapType Code #258(0x102)rrev4-mib
- Port Link Up TrapType Code #259(0x103)rrev4-mib
- Port Link Down TrapType Code #260(0x106)rrev4-mib
- Environmental Temperature Hot TrapType Code #282(0x11A)rrev4-mib
- Environmental Temperature Normal TrapType Code #284(0x11C)rrev4-mib
- IP Event Log Change TrapType Code #1280(0x500)ctip-mib

The following is a list of IP Events that are logged and create the IP Event Log Change Trap.

- IP Routing has been disabled on interface #
- IP Routing has been enabled on interface #
- IP Forwarding has been enabled on interface #
- IP MTU size has been changed on interface #

- IP Framing Type has been changed on interface #
- IP has detected Link UP on interface #
- IP has detected Link DOWN on interface #
- IP Primary address has been changed on interface #
- IP Secondary address has been changed on interface #
- IP Access Control Lists have been enabled on interface #
- IP Access Control Lists have been disabled on interface #
- IP has detected Port UP (WAN devices only)
- IP has detected Port DOWN (WAN devices only)
- IP Proxy ARP has been disabled on interface #
- IP Proxy ARP has been enabled on interface #
- IP RIP has been enabled on interface #
- IP RIP has been disabled on interface #
- IPX Event Log Change Trap Type Code #1281(0x501) ctipx-mib

The following is a list of IPX Events that are logged and create the IPX Event Log Change Trap.

- IPX Routing has been disabled on interface #
- IPX Routing has been enabled on interface #
- IPX Forwarding has been enabled on interface #
- IPX MTU size has been changed on interface #
- IPX Framing Type has been changed on interface #
- IPX has detected Link UP on interface #
- IPX has detected Link DOWN on interface #
- IPX Primary address has been changed on interface #
- IPX Access Control Lists have been enabled on interface #
- IPX Access Control Lists have been disabled on interface #
- IPX has detected Port UP (WAN devices only)

- IPX has detected Port DOWN (WAN devices only)
- IPX RIP has been enabled on interface #
- IPX RIP has been disabled on interface #
- IPX SAP has been enabled on interface #
- IPX SAP has been disabled on interface #

Software and Firmware Upgrades

Software and Firmware upgrades can be performed remotely through the Windows-based QuickSET utility application. Refer to **Chapter 7** for QuickSET instructions. QuickSET allows you to retrieve or upgrade the firmware, software, and configuration files from its **Firmware Upgrade** menu by selecting the **TFTP/BootP Services** window to access a TFTP (Trivial File Transfer Protocol) server.

3

ISDN Line Ordering and Configuration

This chapter provides ISDN BRI (Basic Rate Interface) line ordering and configuration information. It contains the following sections:

- **Arranging ISDN Service**
- **Telephone Switch Support**
- **ISDN BRI Line Configuration**
- **SPIDs, Directory Numbers and Telephone Numbers**
- **Telephone Switch Parameters**

Read the first section in this chapter for an overview of the steps required to order ISDN service from your service provider (telephone company). The rest of the chapter details the information that the service provider needs to give you, and which you need to give to the service provider.

Arranging ISDN Service

The service provider requires certain information about the capabilities of the CSX400. You must give the service provider the required switch settings (parameters) for the provider's central office switch. Consult with your service provider at least two months before you require the installation and use of the ISDN service.

Complete the following steps to arrange your ISDN service:

1. Contact the service provider and determine what type of ISDN central office switches are available (see **Telephone Switch Support** in this chapter).
2. Supply the service provider with the provisioning information for their switch type to enable proper configuration of the ISDN line (see **Telephone Switch Parameters** in this chapter).
3. Once the ISDN line is installed, ensure that the service provider supplies you with the following information:
 - ISDN telephone numbers
 - ISDN Service Profile Identifier numbers (SPIDs) and/or Directory Numbers (DNs) (see **SPIDs, Directory Numbers and Telephone Numbers** in this chapter).

Telephone Switch Support

Your telephone company may offer a variety of ISDN switch types. You must contact your service provider and find out which type of ISDN service is available.

The following switch types are currently supported by the CSX400 within the U.S.:

- **National ISDN 1 (NI-1)**
- **AT&T 5ESS with Custom Software**
- **DMS-100**

Outside of the U.S. the following switch types are currently supported:

- NET3 (European ISDN)
- NET3SW (European Swiss-variant)
- NTT (Nippon Telegraph and Telephone)
- KDD (Kokusai Den shin Denwa Co., Ltd.)
- French Delta (VN4) switches

ISDN BRI Line Configuration

You need to order one Basic Rate Interface (BRI) ISDN line from your service provider. The Basic Rate Interface ISDN line provides two full duplex 64 (Kbps) B channels used for voice, data, fax, etc. and one full duplex 16 Kbps channel used for signaling. Each B channel can be used for a call; i.e., two calls can occur at the same time. Services vary from individual service providers.



Full 64 Kbps for each channel (called clear channel) may not be available across the entire communications link. Today, many providers still use in-band signaling (the 8 Kbps signaling is taken from the B channel bandwidth) so that you may only achieve a 56 Kbps channel speed.

The service provider requires some information from you about your configuration. You must provide your service provider with the required switch settings for the provider's telephone switch (see **Telephone Switch Parameters** in this chapter). Consult with your service provider at least two months before requiring the installation and use of the ISDN service.

In the U.S. and Canada, Network Terminator equipment (NT1) is required to provide an interface between the CSX400 and the ISDN line. The NT1 offers conversion between the two-wire twisted pair (U-loop interface) used by telephone companies and the four-wire terminal equipment (S/T Interface) as well as line-testing capabilities. External Network Terminator equipment comes with a power supply (built-in or external).

In Europe and Japan, the telephone company provides the NT1 and offers end-users the S/T interface. The S refers to a connection between customer equipment in some ISDN configurations when a PBX is present. The T refers to the connection between the NT1 device and the CSX400.

The ISDN pairs are the same wires that exist for analog telephone service. In most cases, the same wires can be used for the ISDN line. The EIA/TIA standard for wiring is Unshielded Twisted Pair (UTP) cable, Category 3 or above, 24 AWG (American Wire Gauge). The standard also recommends using 8-position RJ45 jacks for new ISDN service installation. No special conditioning is required; in some cases, conditioning must be removed.

ISDN BRI Configurations

ISDN BRI lines can be configured in point-to-point and multi-point configurations. With a point-to-point configuration, only one device is connected to the ISDN line. With a multi-point configuration, it is possible to have up to 8 devices (telephones, faxes, routers, etc.) connected to the line.

Since the ISDN BRI line is used for a high speed LAN-to-LAN link, you must ensure that additional devices connected to the S/T interface allow sufficient access for the bandwidth requirements of the CSX400.

SPIDs, Directory Numbers and Telephone Numbers

The service provider gives you up to three sets of numbers for identifying the ISDN line and devices. You may be assigned none, one or two Service Profile Identifier numbers (SPIDs) or Directory Numbers (DNs) depending on the service provider and country.

Phone Numbers

Numbers used for others to dial into the ISDN B channels on your ISDN line (similar to analog line phone numbers).

Directory Numbers

Address assigned by the ISDN service provider for each device operating on the line. This number can be similar to the phone number. The Directory Number is not generally implemented outside the U.S.

Service Profile Identifiers

SPIDs, also assigned by the ISDN service provider, identify the services and features that the telephone company switch provides to the ISDN device. Commonly implemented in the U.S. and Canada, the SPID is often derived from the directory number, combined in a series with other digits. SPIDs are not generally implemented outside the U.S. and Canada.

Telephone Switch Parameters

Once you have contacted your service provider and learned the type of ISDN switch being used, refer to **Table 1**, **Table 2**, and **Table 3**. You must supply the appropriate provisioning information to the service provider to ensure proper configuration of the ISDN line.



National ISDN 1 (NI-1) is a specification released by Bellcore outlining a basic set of ISDN services used for standardization by equipment vendors.

Table 1 National ISDN 1 (NI-1)

ISDN Switch Parameters	Value
B1	Circuit Switched Data & Voice
B2	Circuit Switched Data & Voice
D	Signaling Only
Multipoint	Yes
Terminal Type	A
Display	Off
TEI	Dynamic
MTERM	1
MAXB CHL	2
ACT USR	Y
CSD	2
CSD CHL	Any

Table 1 National ISDN 1 (NI-1) (Continued)

ISDN Switch Parameters	Value
CSD Limit	2
CA Pref	1
EKTS	No
Nail Up	None

Table 2 AT&T 5ESS with Custom Software

ISDN Switch Parameters	Value
B1	Circuit Switched Data & Voice
B2	Circuit Switched Data & Voice
D	Signaling Only
Multipoint	No
Terminal Type	A
Display	Off
TEI	Dynamic
MTERM	1
MAXB CHL	2
ACT USR	Y
CSD	2
CSD CHL	Any
CSD Limit	2
CA Pref	1
Nail Up	None

Table 3 DMS-100

ISDN Switch Parameters	Value
B1	Circuit Switched Data & Voice
B2	Circuit Switched Data & Voice
D	Signaling Only
EKTS	No
Ringing Indicator	No
Release Key	No
PVER	01
TEI	Dynamic
MAXKEYS	64
Nail Up	None

4

Planning for CSX400 ISDN Configuration

This chapter explains the CSX400 ISDN-BRI configuration process and terminology. It also describes the information that is required for configuration.

Configuration Process and Terminology

During configuration, you specify information identifying the CSX400 and define the LAN and WAN connections of the CSX400. All of the remote routers to which this device may connect are added to a database called the remote router database that resides in the CSX400. Each remote router entry in the database defines the connection parameters, security features, route addressing and bridging function for the remote router (see the example in [Figure 2](#)). Routing and bridging are controlled by specific remote router entry information as well as general controls that are set after all other information is configured.

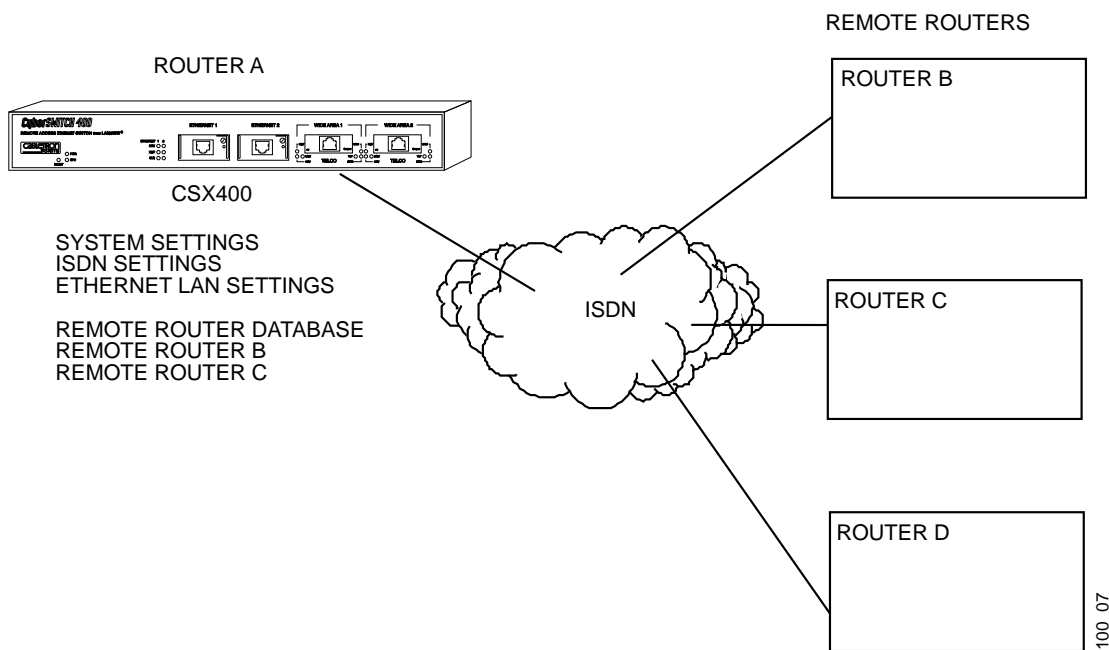


Figure 2 Router A Configuration

Collect Network Information

Before you begin, you need to obtain information about the network to which you are adding the CSX400. Some of the information is obtained from your central site or remote site network administrator. Other information is obtained from your ISDN service provider.

You must define the name and security password of the CSX400, ISDN line information and the Ethernet LAN IP and/or IPX address. You need to identify all of the remote routers and their routing and bridging capability, ISDN phone numbers, addressing and security information. You also need to decide whether you will use Internet Firewall Filtering if you are using IP routing. The following sections contain diagrams and tables to help you gather and organize the information.

Names and Passwords

You must choose a name for the CSX400 and the authentication password, both of which are used by a remote site to authenticate the target router. For each remote router, you must have the router name and its authentication password which is used by the CSX400 to authenticate the remote router. The name and password are used in both PAP and CHAP authentication. **Figure 3** shows how this information is used.

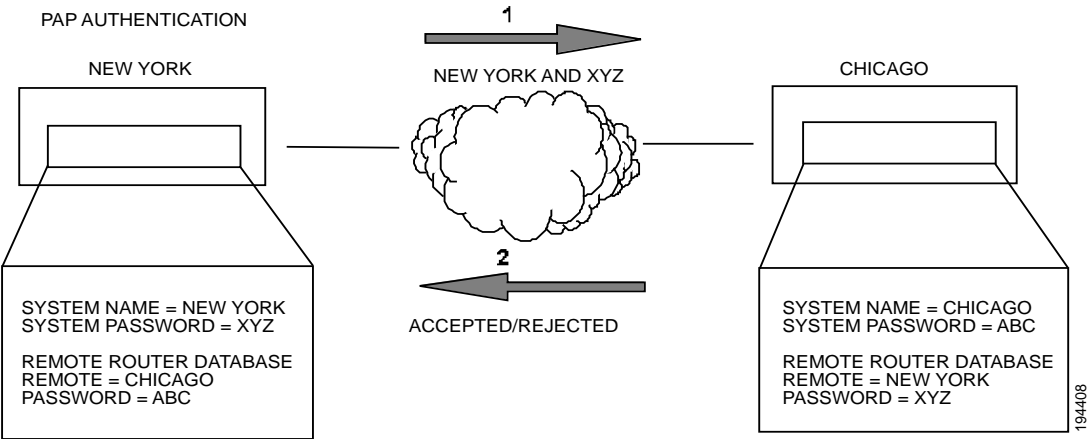


Figure 3 PAP Authentication

ISDN Line Information

You need to know the telephone switch type and phone numbers associated with the ISDN line. The telephone switch types supported are listed in **Telephone Switch Support**. The service provider gives you up to three sets of numbers for identifying the ISDN line and attached devices. You may be assigned none, one or two SPIDs or DNs and this varies by service provider and country.

Phone Numbers — Numbers used for others to dial into the ISDN B channels on your ISDN line (similar to analog line phone numbers).

Directory Numbers — Address assigned by the ISDN service provider for each device operating on the line. This number can be similar to the phone number. The Directory Number is not generally implemented outside the U.S.

Service Profile Identifications — SPIDs, also assigned by the ISDN service provider, identify the services and features that the switch provides to the ISDN device. Commonly implemented in the U.S. and Canada, the SPID is often derived from the directory number, combined in a series with other digits as shown in the example in **Figure 4**. SPIDs are not generally implemented outside of the U.S. and Canada.

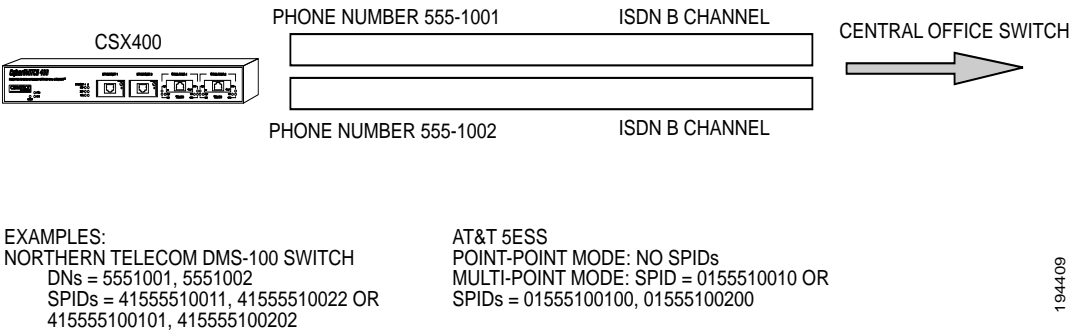
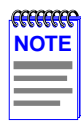


Figure 4 Service Profile Identifications (SPIDs)

Refer to **Chapter 3, ISDN Line Ordering and Configuration**, for further information about ISDN configurations and line ordering.

Network Information Diagrams

It is helpful to draw a diagram including all locations, addresses, router names, etc. This section includes diagrams needed to configure the CSX400. You may need different addressing information depending on whether you are configuring IP routing and/or NetWare IPX routing.



The diagrams show the information required to configure only the CSX400. If you need to configure both ends of the WAN link, you should label all information for the network.

TCP/IP Routing — An IP address and subnet mask are required for the Ethernet LAN for the router connection. Each remote router ISDN WAN link may have local and remote IP addresses and subnet masks depending on the type of IP addressing as shown in **Figure 5**. The IP routing table in the CSX400 can be “seeded” with addressing information for networks/stations beyond the remote router.

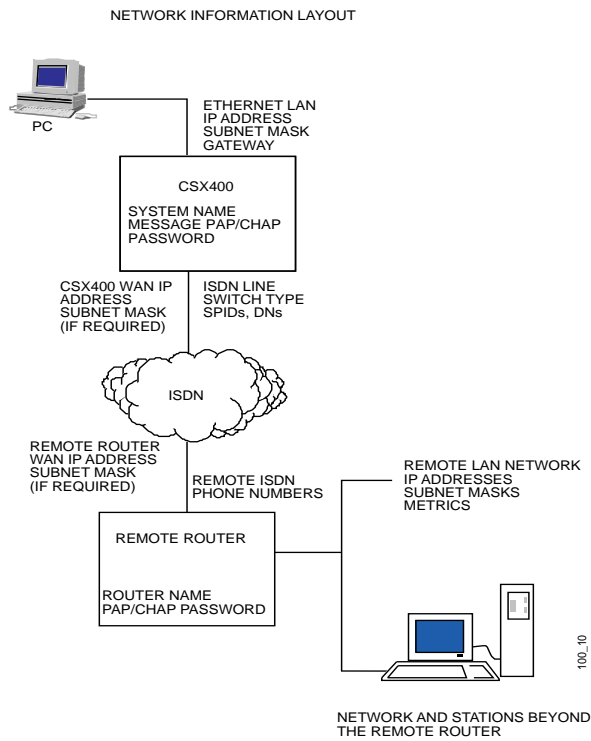


Figure 5 Network Information Layout

TCP/IP Route Addresses — If the CSX400 is to direct traffic to networks or stations beyond the remote router, the routing table in the CSX400 can be “seeded” with static IP routes. An IP route includes an IP address, subnet mask and metric. The metric is a number representing the perceived cost in reaching the remote network or station.

The CSX400 routing table must be seeded statically so that it dials out to the appropriate remote router when IP traffic is targeted to networks and stations beyond that remote router. After the link is established, RIP update packets are dynamically added to the routing table. Seeding the routing table is not necessary when the CSX400 never dials out; it discovers remote networks and stations beyond the calling router as soon as RIP updates arrive (provided the remote router supports RIP and RIP packets are allowed to flow on the WAN link).

TCP/IP Default Route — One default route should be designated in the routing table for all traffic that cannot be directed to other specific routes. You need to define the default route for a remote router if the CSX400 will be placing calls to that remote router.

Source (Target) and Remote WAN IP Addresses — You may need to specify a Source WAN IP address and/or a Remote WAN IP address for the WAN connection to the remote router depending on IP address negotiation under PPP. Check with your system administrator for details on whether the router must communicate in numbered or unnumbered mode and what addresses are required.

In unnumbered mode, neither IP address is defined on the link. In numbered mode, one IP address is defined on each end of the WAN link. These addresses may or may not belong to the same subnetwork. They may also be determined automatically, negotiated, or forced by the network administrator.

The CSX400 automatically determines whether to run in unnumbered mode or numbered mode. If unnumbered mode negotiation fails, numbered mode is attempted using the Ethernet LAN IP address as a default. If you have specified a Source WAN IP address, unnumbered mode negotiation is not performed; i.e., the operating mode is numbered. If a Source WAN IP address is explicitly defined, the router will not, as a rule, accept another local address from the remote end. In numbered mode without an explicit Source WAN IP address, this address can be negotiated to a different value by the remote end.

Planning for CSX400 ISDN Configuration

If the remote router supports unnumbered mode, neither address needs to be specified. **Figure 6** provides a simple example of an unnumbered mode configuration.

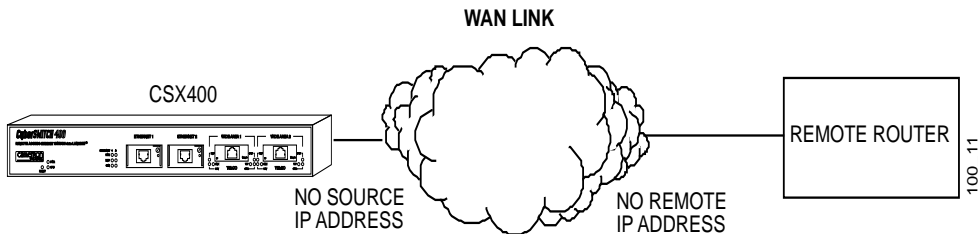


Figure 6 CSX400 in Unnumbered Mode

For numbered mode, consider the capabilities of the remote router as well as your requirements. Specify a Source WAN IP address if the CSX400 must be on the same subnetwork as the remote router. **Figure 7** is an example of a Class B IP network (128.1).

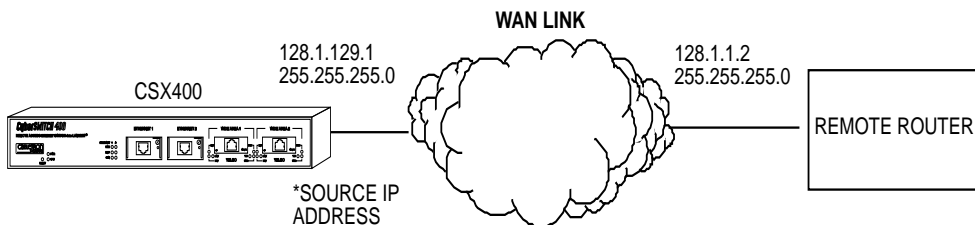
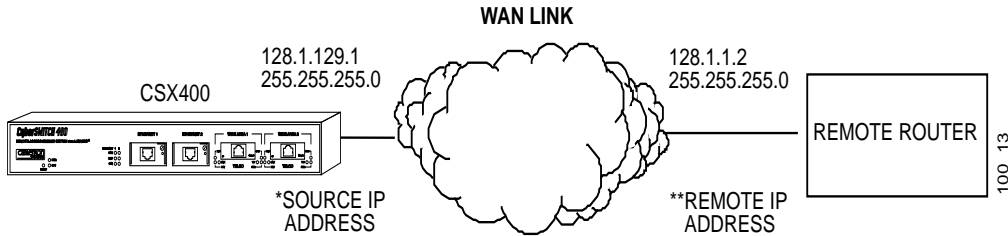


Figure 7 CSX400 in Numbered Mode on the Same Subnetwork as the Remote Router

Specify a Remote WAN IP Address if the remote router does not support IP address negotiation under PPP (i.e., does not have a pre-assigned IP address as shown in **Figure 8**).



*SPECIFY SOURCE IP ADDRESS IF IT MUST BE ON SAME SUBNETWORK AS THE REMOTE ROUTER.

**SPECIFY REMOTE IP ADDRESS IF REMOTE ROUTER DOES NOT HAVE A PRE-ASSIGNED IP ADDRESS.

Figure 8 CSX400 to Remote Router Without a Pre-Assigned IP Address

NetWare IPX Routing — An Ethernet LAN IPX network number is required for the CSX400 local Ethernet LAN connection. The ISDN WAN link to each remote router must have an assigned IPX network number. IPX Routes and IPX SAPs for each remote router are also required for the configuration process. **Figure 9** provides an example of the network layout for IPX routing.

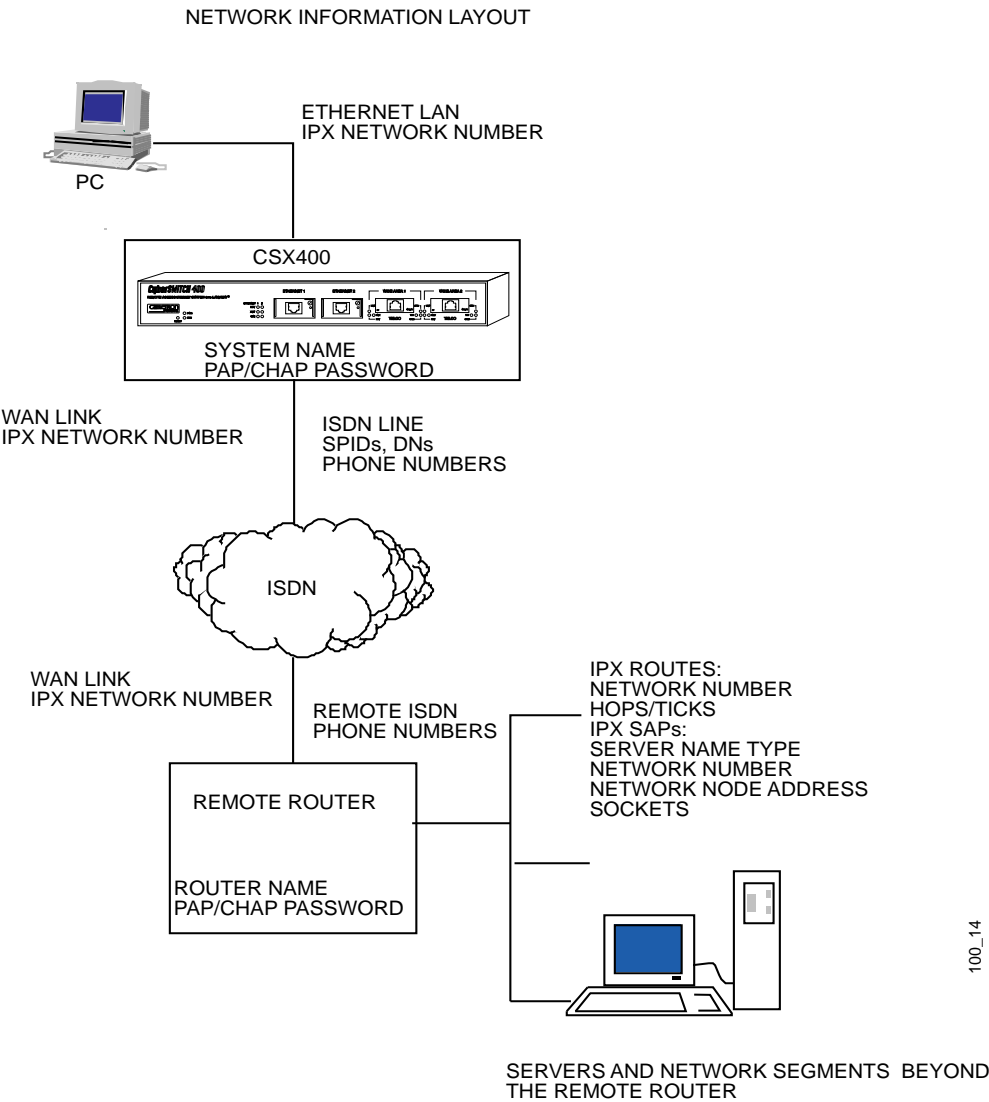


Figure 9 Network Information Layout

IPX Routes — If the CSX400 is to direct traffic to network segments and servers beyond the remote router, the routing table in the CSX400 can be “seeded” with static IPX routes. An IPX route includes a network number, hop count and ticks. The hop count is the number of routers through which traffic must pass to reach the remote network segment or server. Ticks represent how much time the packet takes to reach the destination in roughly 1/18th of a second increments.

The CSX400 routing information table must be seeded statically so that it dials out to the appropriate remote router when IPX traffic is targeted to network segments or servers beyond that remote router. After the link is established, RIP update packets dynamically add to the routing information table in the CSX400. Seeding the routing table is not necessary when a CSX400 never dials out; it will discover routes beyond the calling router as soon as RIP updates arrive (provided the remote router supports RIP).

IPX SAPs — If the CSX400 is to obtain services beyond the remote router, the CSX400 SAP services table must be seeded statically. A SAP service is identified by a server name and corresponding server type, network number, node number and socket. The socket number represents the service (application) within the server node.

The CSX400 SAP services table must be seeded statically so that the device can direct traffic to the appropriate remote router when a service is requested from a server beyond that remote router. After the link is established, SAP broadcast packets dynamically add to the target router services table. Seeding the table is not necessary when a CSX400 never dials out; it will discover remote services beyond the calling router as soon as SAP broadcasts arrive (provided the remote router supports IPX).

IPX Network Numbers — IPX network numbers are assigned to LAN network segments as well as servers. These numbers should be unique for all IPX networks on the Internetwork.

IPX external network numbers refer to the physical LAN network segments to which servers and routers are connected. The WAN link network number is an external IPX network number. This is a unique number that you choose (or are given by the network administrator) to represent the WAN link between the CSX400 and remote router. The local Ethernet IPX network number is also an external network number.

Servers are identified with internal network numbers. This is a logical network number that identifies the individual server. For a local router to access a server beyond the remote router, you specify a route using the internal network number of a server. To seed the routing table to access a network segment, you specify the external network number of the LAN segment. The network number in the SAP table is the internal network number of the server.

Node Numbers — Servers can have internal and external node numbers. The internal node number is a logical number assigned by the system administrator to the server. The external node number is the MAC address of the server. When adding SAP services to the SAP table, internal node numbers are used.

Network Information Tables

The following tables list the items you need to define or obtain to configure the router. This information is illustrated in the network information diagrams and described in the previous sections. Worksheets are provided in **Chapter D**, so that you can enter details about your CSX400 and remote routers. **Table 4** provides information for configuring your system settings, **Table 5** explains the Remote Router Database configuration settings and **Table 6** details bridging and routing configuration.



To configure the CSX400, you need to fill out one chart for the CSX400 and one Remote Router chart for each remote router to be entered into the remote router database. If you are setting up both ends of the network, you need a mirror image of the information listed below for configuring the router on the other end of the ISDN link.

Table 4 Configuring System Settings

Configuration Section	Item	Description
System Settings	Router Name	Name used to identify this router; sent to other routers during PAP/CHAP security authentication and displayed in the Configuration Manager window.
	Message	Message saved in the router to be read by a system administrator; displayed on the Configuration Manager main menu window.
System Settings Dial Authentication Password	Dial Authentication Password/Secret	This router's password used for authentication when the router dials out to other routers or is challenged by them.

Table 4 Configuring System Settings (Continued)

Configuration Section	Item	Description
System Settings ISDN Settings	ISDN Line Numbers (supplied by the service provider)	SPIDs and Directory Numbers for one or two ISDN B-Channels
	Type of Telco switch	NTT Nippon Telegraph/Telephone KDD Kokusai Denshin Denwa Co. NI-1 National ISDN 1 AT&T 5ESS w/Custom Software Northern Telecom DMS-100 NET3 European ISDN NET3SW Swiss-Variant ISDN
System Settings Ethernet IP Address	Ethernet IP Address and Subnet Mask	Address and Subnet Mask for Ethernet port Connection
System Settings Ethernet IPX Network #	Ethernet IPX Network Number	Network Number for Ethernet port connection

Table 5 Configuring the Remote Router Database

Remote Router Configuration Database	Item	Description
Dial Settings	ISDN Line	ISDN Phone Numbers for one or two ISDN B-Channels
	Disconnect Timer	Disconnect link on inactivity timeout
	Maximum Links	Maximum number of links for bandwidth on demand (1 or 2)
	Minimum Links	Minimum links (0, 1, or 2)
	Threshold	Percent Bandwidth utilization threshold
	Bandwidth Direction	Management on IN OUT BOTH
Dial-In Security	PAP CHAP Security Procedure	PAP CHAP NONE; minimum level of authentication required for the remote router.
	Password/Secret	The remote router's password used for authentication when it dials the target router or is challenged by the target router.
Bridging On/Off	Bridging On/Off	Bridging from/to the remote router is On or Off.
	Spanning Tree Protocol	On or Off

Table 5 Configuring the Remote Router Database (Continued)

Remote Router Configuration Database	Item	Description
TCP/IP Route Addresses	IP Address, Subnet Mask, and Metric	IP Address, Subnet Mask of the remote network beyond the remote router; specifies metric for calculating route efficiency.
	Remote WAN IP Address and Subnet Mask ^a	IP Address and Subnet Mask of the Remote Router's end of the WAN link.
	Source WAN IP Address and Subnet Mask ^b	IP Address and Subnet Mask of the local end of the WAN link.
IPX Routes	IPX Routes: Network Number, Hop Count and Ticks	IPX Network Number, Hop Count and Ticks for stations/nodes beyond the remote router. Hop count is number of routers to pass through and ticks is time delay (each 1/18th of a second).
IPX SAPs	SAPs: Server Name, Server Type, Network Number, Node Number and Socket	Information defining application services available on stations/nodes beyond the remote router.
	WAN Network Number	Network Number for the WAN link between target router and remote router

- a. Used only in PPP numbered mode of addressing
- b. Used only in PPP numbered mode of addressing



Make one chart for each remote router in the remote router database.

Table 6 Bridging and Routing Controls

Bridging/Routing Configuration Database	Item	Description
Bridging/Routing	Remote Bridging Destination	Destination dialed when bridging any outbound data traffic (required for outbound bridging)
	TCP/IP Routing	TCP/IP routing to all destinations On or Off
	NetWare IPX Routing	IPX routing to all destination On or Off
	Internet Firewall	Internet Firewall active or not

Sample Configuration

A sample configuration of a hypothetical network is provided in this section. **Figure 10** depicts a small office (FP2) accessing a central site (FP3) via an ISDN link. The small office also has access to Internet through an Internet Service Provider (ISP).

The small office and central site have IP routing with a Class B addressing scheme and IPX routing. Bandwidth-on-demand is configured for accessing central site FP3. A maximum of one line is configured for calling the ISP (though two different phone numbers are defined for use). **Table 7** provides sample system settings, **Table 8** provides sample settings for the remote router at the FP3 site, **Table 9** provides sample settings for the remote router at the ISP site and **Table 10** provides sample bridging and routing settings.

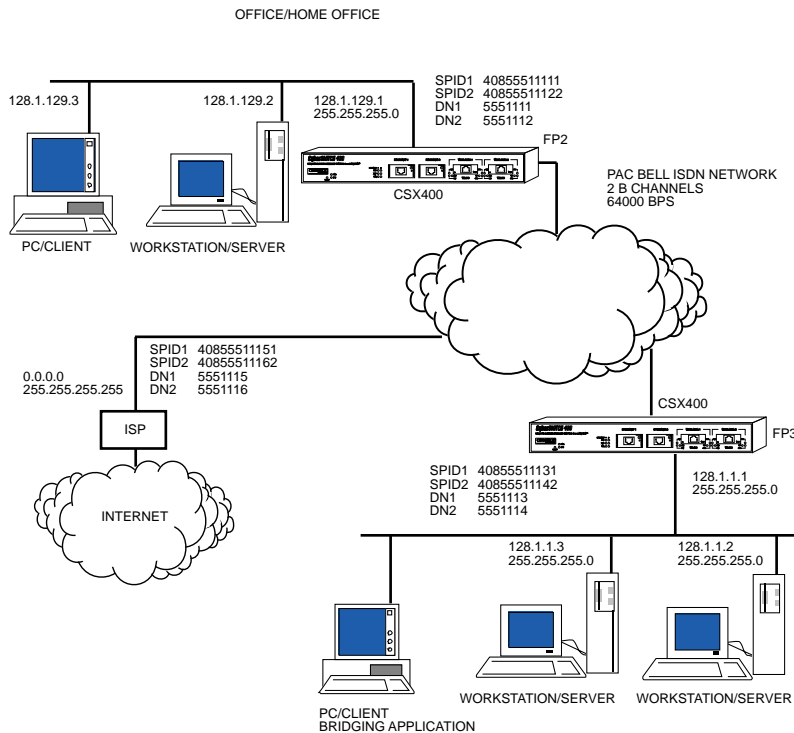


Figure 10 Sample Network Diagram

Table 7 CSX400 Sample Configuration Settings

Configuration Section	Item	Setting
System Settings	Router Name	FP2
	Message	Configured_Mar_1996
System Settings Dial Authentication Password	Dial Authentication Password/Secret	FP2passwd
System Settings ISDN Settings	ISDN SPID#1	40855511111
	ISDN SPID#2 ISDN	40855511122
	Directory Number #1	DN1 5551111
	ISDN Directory Number #2 ISDN	DN2 5551112
	Switch Type	DMS-100
System Settings Ethernet IP Address	Ethernet IP Address and Subnet Mask	128.1.129.1 255.255.255.0
System Settings Ethernet IPX Network #	Ethernet IPX Address: Network Number	123

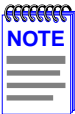
Table 8 Remote Router: FP3

Configuration Section	Item	Setting
Remote Router Database Dial Settings	ISDN Phone #1	5551113
	ISDN Phone #2	5551114
	Disconnect Timer Value	60
	Maximum Links	2
	Minimum Links	0
	Threshold	75
	Bandwidth Direction	BOTH
Remote Router Database Dial-In Security	Minimum Authentication Remote Router's Password/Secret	NONE
Remote Router Database Bridging	Bridging On/Off	ON
	Spanning Tree Protocol	OFF
Remote Router Database TCP/IP Route Addresses	Remote Network's IP Addresses, Subnet Masks, and Metrics	128.1.0.0 255.255.0.0 1
	Source WAN IP Address and Subnet Mask ^a	Not required
	Remote WAN IP Address and Subnet Mask ^b	Not required

Table 8 Remote Router: FP3 (Continued)

Configuration Section	Item	Setting
Remote Router Database NetWare IPX Routes	IPX Address: Network Number, Hop Count and Ticks	1001 1 4
Remote Router Database NetWare IPX SAPs	SAPs: Server Name, Server Type, Network Number, Node Number and Sockets WAN Network Number	Serv312_fp 4 1001 00-00-00-00-00-01 451 789

- a. Used only in PPP numbered mode of addressing
- b. Used only in PPP numbered mode of addressing



Use one chart for each remote router in the remote router database.

Table 9 Remote Router: ISP (Internet Service Provider)

Configuration Section	Item	Setting
Remote Router Database Dial Settings	ISDN Phone #1	5551115
	ISDN Phone #2	5551116
	Disconnect Timer Value	Default (60 seconds)
	Maximum Links	Default (1)
	Minimum Links	Default (0)
	Threshold	Default (0)
	Bandwidth Direction	Default (Both)
Remote Router Database Dial-In Security	Minimum Authentication	PAP
	Remote Router's Password/Secret	ISPpasswd

Table 9 Remote Router: ISP (Internet Service Provider) (Continued)

Configuration Section	Item	Setting
Remote RouterDatabase Bridging	Bridging On/Off	Bridging OFF
	Spanning Tree Protocol	OFF
Remote Router Database TCP/IP Routes	Remote Network's IP Addresses, Subnet Masks, and Metrics	0.0.0.0 255.255.255.255 1
	Source WAN IP Address and Subnet Mask ^a	Not required
	Remote WAN IP Address and Subnet Mask ^b	Not required
Remote Router Database NetWare IPX Routes	IPX Address: Network Number, Hop Count and Ticks	Not required
Remote Router Database NetWare IPX SAPs	SAPs: Server Name, Server Type, Network Number, Node Number and Sockets	Not required
	WAN Network Number	Not required

a. Used only in PPP numbered mode of addressing

b. Used only in PPP numbered mode of addressing



Use one chart for each remote router in the remote router database.

Table 10 Bridging and Routing Controls

Configuration Section	Item	Setting
Bridging and Routing	Default Remote Bridging Destination	FP3
	TCP/IP Routing On/Off	ON
	NetWare IPX Routing On/Off	ON
	Internet Firewall On/Off	ON

Names and Passwords Example

In the sample configuration provided in **Table 11**, a small office FP2 communicates with a central site FP3 and an Internet Service Provider ISP. As indicated in this example, router FP2 has a system password “FP2passwd”. This password is used when FP2 dials out to site FP3 for authentication by that site, and at any time when FP3 challenges FP2. FP3 has a system password “FP3passwd” which is, likewise, used when FP3 dials out to site FP2 for authentication by FP2, and at any time FP2 challenges FP3. The ISP site has a system password “ISPpasswd” used for the same purpose.

Each router includes the remote router password in the definition of any remote site to which it communicates. The router will use the remote password to authenticate the remote site when the remote router dials in or is challenged by the local site. For example, FP2 has remote router entries for FP3 and ISP, and defined in each entry are the respective remote router password.

The following table shows the names and passwords for each router that must be defined for authentication to be performed correctly. (This assumes that all three systems use some form of authentication protocol.)

Table 11 Router Names and Passwords

System Name: FP2 Router	
System Password	FP2passwd
Remote Router Database	
Remote Router FP3 Remote's Password	FP3passwd
Remote Router ISP Remote's Password	ISPpasswd

System Name: FP3 Router	
System Password	FP3passwd
Remote Router Database	
Remote Router FP2 Remote's Password	FP2passwd

System Name: ISP Router	
System Password	ISPpasswd
Remote Router Database	
Remote Router FP2 Remote's Password	FP2passwd

5

Ethernet Cabling Requirements

This chapter contains general networking guidelines. Before attempting to install the CSX400 or any additional EPIMs or WPIMs, review the requirements and specifications outlined in this chapter.



Your network installation must meet the conditions, guidelines, specifications, and requirements included in this chapter to ensure satisfactory performance of this equipment. Failure to follow these guidelines may result in poor network performance.

Network Requirements

Take care in planning and preparing the cabling and connections for your network. The quality of the connections, the length of cables, and other conditions of the installation play critical roles in determining the reliability of your network.

This chapter contains general guidelines for the following:

- 10BASE-T Twisted Pair Network
- Multimode Fiber Optic Network
- Single Mode Fiber Optic Network
- 10BASE2 Coaxial Cable Network
- Transceiver Requirements

Refer to the following sections that apply to your specific network configuration.

10BASE-T Twisted Pair Network

When connecting a 10BASE-T segment to either of the CSX400 Ethernet interfaces (Twisted Pair Ethernet Port Interface Module [EPIM-T]), ensure that the network meets the following requirements:

Length — The IEEE 802.3 10BASE-T standard requires that 10BASE-T devices transmit over a 100 meter (328 foot) link using 22–24 AWG unshielded twisted pair wire. However, cable quality largely determines maximum link length. If you use high quality, low attenuation cable, you can achieve link lengths of up to 200 meters. Cable delay limits the maximum link length to 200 meters.



Losses introduced by connections at punch-down blocks and other equipment reduce total segment length. For each connector or patch panel in the link, subtract 12 meters from the total length of the cable.

Insertion Loss — Between frequencies of 5.0 and 10.0 MHz, the maximum insertion loss must not exceed 11.5 dB. This includes the attenuation of the cables, connectors, patch panels, and reflection losses due to impedance mismatches in the link segment.

Impedance — Cabletron Systems 10BASE-T products work on twisted pair cable with 75-to-165 ohms impedance. Unshielded twisted pair cables typically have an impedance of between 85 and 110 ohms. You can also use Shielded Twisted Pair cables, such as IBM Type 1 cable, but this cable has an impedance of 150 ohms.

Jitter — Intersymbol interference and reflections can cause jitter in the bit cell timing, resulting in data errors. 10BASE-T links must not generate more than 5.0 ns of jitter. Make sure the cable meets 10BASE-T link impedance requirements to rule out jitter as a concern.

Delay — The maximum propagation delay of a 10BASE-T link segment must not exceed 1000 ns. This 1000 ns maximum delay limits the maximum link segment length to no greater than 200 meters.

Crosstalk — Signal coupling between different cable pairs within a multi-pair cable bundle causes crosstalk. 10BASE-T transceiver design alleviates concerns about crosstalk, provided the cable meets all other requirements.

Noise — Crosstalk, or externally induced impulses, can cause noise. Impulse noise may cause data errors if the impulses occur at very specific times during data transmission. Generally, noise is not a concern. If you suspect noise-related data errors, you may need to reroute the cable or eliminate the source of the impulse noise.

Temperature — Multi-pair PVC 24 AWG telephone cables typically have an attenuation of approximately 8–10 dB/100 m at 20°C (68°F). The attenuation of PVC insulated cable varies significantly with temperature. At temperatures greater than 40°C (104°F), Cabletron Systems strongly recommends using plenum-rated cable to ensure attenuation remains within specification.

Multimode Fiber Optic Network

When connecting a multimode fiber optic link segment to the CSX400 (using an EPIM-F1/F2), ensure that the network meets the following requirements:

Cable Type — Use the following multimode fiber optic media:

- 50/125 μm fiber optic cabling
- 62.5/125 μm fiber optic cabling
- 100/140 μm fiber optic cabling

Attenuation — Test the fiber optic cable with a fiber optic attenuation test set adjusted for an 850 nm wavelength. This test verifies that the signal loss in a cable falls within the following acceptable levels:

- 13.0 dB or less for a 50/125 μm fiber cable segment
- 16.0 dB or less for a 62.5/125 μm fiber cable segment
- 19.0 dB or less for a 100/140 μm fiber cable segment

Budget and Propagation Delay — When you determine the maximum fiber optic cable length to incorporate fiber runs into the network, calculate and consider the fiber optic budget (a total loss of 11.0 dB or less is permissible between stations) and total network propagation delay.

To determine the fiber optic budget, combine the optical loss due to the fiber optic cable, in-line splices, and fiber optic connectors. Typical loss for a splice and connector (together) equals 1 dB or less.

Network propagation delay is the amount of time it takes a packet to travel from the sending device to the receiving device. Total propagation delay allowed for the entire network must not exceed 25.6 μ s in one direction (51.2 μ s round trip). If the total propagation delay between any two nodes on the network exceeds 25.6 μ s, you must use bridges or switches.

Length — The maximum possible multimode fiber optic cable length is 2 km (1.24 miles). However, IEEE 802.3 FOIRL specifies a maximum of 1 km (0.62 miles).

Single Mode Fiber Optic Network

When connecting a single mode fiber optic link segment to the CSX400 (using an EPIM-F3), ensure that the network meets the following requirements:

Cable Type — Fiber optic link segments should consist of 8/125 or 12/125 μ m single mode fiber optic cabling. You can also use 62.5/125 μ m multimode cable with the EPIM-F3; however, multimode cable allows for greater optical loss, and limits the possible distance to 2 km.

Attenuation — Test the fiber optic cable with a fiber optic attenuation test set adjusted for a 1300 nm wavelength. This test verifies that the signal loss in a cable falls within the acceptable level of 10.0 dB or less for any given single mode fiber optic link.

Budget and Propagation Delay — When you determine a maximum fiber optic cable length, you must calculate and consider the fiber optic budget (a total loss of 10.0 dB or less between stations) and total network propagation delay.

To determine the fiber optic budget, combine the optical loss due to the fiber optic cable, in-line splices, and fiber optic connectors. Typical loss for a splice and connector (together) equals 1 dB or less.

Network propagation delay is the amount of time it takes a packet to travel from the sending device to the receiving device. Total propagation delay for the entire network must not exceed 25.6 μ s in one direction (51.2 μ s round trip). If the total propagation delay exceeds 25.6 μ s, you must use bridges or switches to re-time the signal.

Length — If your network meets all system budgets, the maximum single mode fiber optic cable length can reach 5 km (3.1 miles) with bridges or switches at each segment end. The FOIRL specifies a maximum of 1 km (0.62 miles).

10BASE2 Coaxial Cable Network

When connecting a thin coaxial cable segment to the CSX400 (using an EPIM-C), ensure that your network meets the following requirements:

Cable Type — Use only 50-ohm RG 58A/U type coaxial cable for thin coaxial cable segments.

Length — The thin coaxial cable segment must not exceed 185 meters.

Terminators — Terminate each end of a thin coaxial cable segment.

Connectors — You can use up to 29 T-connectors throughout the length of the cable segment for host connections. Ensure that all connections are spaced 0.5 meters or more from one another or from terminators.

If you use an excessive number of barrel connectors within the cable segment (e.g., finished wall plates with BNC feed-throughs), you may need to reduce the number of host connections. For special network design information, contact Cabletron Systems Technical Support.

Grounding — For safety, ground only *one* end of a thin coaxial cable segment. Do NOT connect EPIM BNC ports to earth ground.



Connecting a thin coaxial cable segment to earth ground at more than one point could produce dangerous ground currents.

Transceiver Requirements

When you connect an external network segment to an EPIM-A in your CSX400 through a transceiver, that transceiver must meet IEEE 802.3 standards or Ethernet version 1.0 or 2.0 requirements. The transceiver must also have SQE disabled.

6

Installation

This chapter outlines the procedure for attaching the CSX400 to the network. Ensure that the network meets the guidelines and requirements outlined in **Chapter 5, Ethernet Cabling Requirements**, before installing the CSX400. To install the HSIM and WPIMs, you need the following items:

- Antistatic wrist strap (provided with the CSX400)
- Phillips screwdriver

Unpacking the CSX400

Unpack the CSX400 as follows:

1. Remove the shipping material from the box and carefully remove the CSX400.
2. Visually inspect the CSX400. If there are any signs of damage, contact Cabletron Systems (refer to the **Getting Help** section) immediately.
3. Read the *CSX400 Release Notes* included in the shipping box.

Guidelines for Installations



Only qualified personnel should perform installation procedures.



Do not connect EPIM ports to the Public Switched Telephone Network (PSTN). Hazardous voltages exist that may damage the CSX400.

Installation sites must be within reach of the network cabling and meet the requirements listed below:

- A properly grounded power receptacle must be within seven feet of the location.

Installation

- In a shelf installation, the shelf must be able to support 13.6 kg (30 lb) of static weight for each device on the shelf.
- Maintain a temperature of between 5°C (41°F) and 40°C (104°F) at the installation site with fluctuations of less than 10°C (50°F) per hour.
- Maintain a two-inch clearance for each side and the back of the device for adequate ventilation.

Installing Interface Modules

Depending on your specific application, install Cabletron Systems WAN Port Interface Modules (WPIMs) and the CSX-COMP/ENCR modules into the CSX400 before proceeding with the installation of your CSX400. Refer to the **Installing Ethernet Port Interface Modules (EPIMs)**, **Installing WAN Port Interface Modules (WPIMs)**, and **CSX-COMP/ENCR Installation** sections within this chapter for installation instructions.



The EPIMs and WPIMs, and CSXCOMP/ENCR for the CSX400 are sensitive to static discharges. Use a grounding strap and observe all static precautions during installation. Failure to do so could result in damage to the EPIMs, WPIMs, CSXCOMP/ENCR, and the CSX400.



The CSX400 must have at least one EPIM and one WPIM installed before you can begin configuring the device.

Installing Ethernet Port Interface Modules (EPIMs)

This section contains procedures for adding or replacing an Ethernet Port Interface Module (EPIM) to upgrade or change the capabilities of your CSX400. After installing your new EPIM, refer to **Chapter 5, Ethernet Cabling Requirements**, for network configuration guidelines. **Appendix A, EPIM Specifications**, provides specification information on Cabletron Systems EPIMs.



Before performing installation procedures, ensure that the requirements outlined in the section, **Guidelines for Installations**, are met.

To install an EPIM, perform the following steps:



When removing an existing EPIM, make sure to pull the module straight out to avoid damaging the connector.

1. Attach the disposable grounding strap to your wrist (refer to the instructions outlined on the disposable grounding strap package).
2. Remove the coverplate or the existing EPIM (whichever applies).
3. Slide your new EPIM into place, making sure the connectors on the rear of the module and inside the CSX400 attach properly as shown in **Figure 11**.
4. Install the mounting screw.

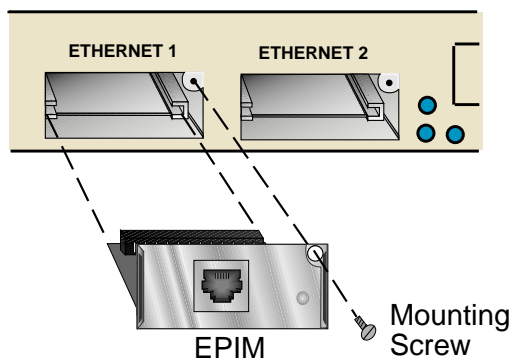


Figure 11 Installing an EPIM

Removing the CSX400 Cover

This section describes how to remove the CSX400 chassis cover. The cover must be removed to install a WAN Port Interface Module.



DO NOT REMOVE THE COVER FROM THE CSX400 WHILE POWER IS APPLIED TO THE UNIT.

DO NOT POWER UP THE DEVICE AGAIN UNTIL THE COVER AND SCREWS ARE IN PLACE.

DECKEL VON DAS CSX400 NICHT ABZIEHEN UNTER SPANNUNG.

CSX400 NICHEINSCHALTEN SO LANG DER DECKEL UND SCHRAUBEN NICHT EINGEBAUT SIND.

NO DEBE DE REMOVER LA TAPA DURENTE QUE ESTE CONELTADO A LA CORRIENTE.

NO ENCHUFE A LA CORRIENTE HASTA QUE LA TAPA Y LOS TORNILLOS ESTEN EN SU LUGAR.

To remove the chassis cover, proceed as follows:

1. Disconnect the CSX400 from the network as follows:

- a. Unplug the power cord from the rear of the CSX400 chassis.



Before performing **step b**, mark any cables connected to the CSX400 according to their associated port numbers. This is recommended for ease of reinstallation.

- b. Disconnect all network cables attached to the CSX400.
2. Use a Phillips screwdriver to remove the seven screws that attach the chassis cover to the unit. Place the screws aside. (See **Figure 12**).
 3. While facing the back of the unit, remove the chassis cover by pulling the cover toward you and then up.

Removing the CSX400-DC Cover

This section describes how to remove the CSX400-DC chassis cover. The cover must be removed to install a WAN Port Interface Module (WPIM).



Do not remove the cover from the CSX400-DC while power is applied to the unit. Do not power up the device again until the cover and screws are in place.

To remove the chassis cover, proceed as follows:

1. Disconnect the CSX400-DC from the network as follows:
 - a. Flip the DC switch located in the back of the CSX400-DC to the “off” position.



Before performing step b, mark any cables connected to the CSX400-DC according to their associated port numbers. This is recommended for ease of reinstallation.

- b. Disconnect all network cables attached to the CSX400-DC.
2. Use a Phillips screwdriver to remove the seven screws that attach the chassis cover to the unit. Place the screws aside. (See **Figure 12**).
3. While facing the back of the unit, remove the chassis cover by pulling the cover toward you and then up.

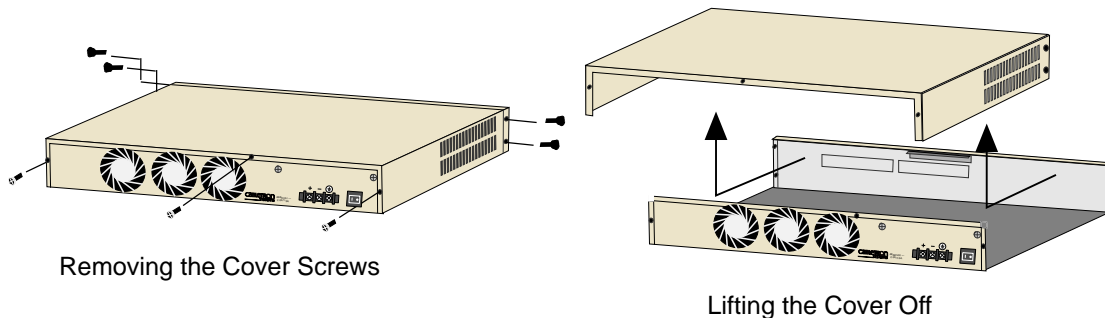


Figure 12 Removing the Chassis Cover

Installing WAN Port Interface Modules (WPIMs)



Before performing installation procedures, ensure that the requirements outlined in the section, **Guidelines for Installations**, are met.

To install a WPIM into the CSX400, refer to **Figure 13** and complete the following steps:



When removing an existing WPIM, make sure to pull the module straight out to avoid damaging the connector.

1. Attach the disposable grounding strap to your wrist (refer to the instructions outlined on the disposable grounding strap package).
2. Remove the CSX400 cover (refer to **Removing the CSX400-DC Cover** for instructions).
3. Remove the blank faceplate from the appropriate WAN slot.
4. Orient the WPIM as shown in **Figure 13**.
5. Carefully insert the WPIM connector into the WPIM connector pins on the CSX400.
6. Press down firmly on the WPIM until the pins slide all the way into the connector. Ensure that the WPIM seats flush on the standoffs.
7. Secure the WPIM to the three standoffs using the provided screws.
8. Replace the CSX400 cover.

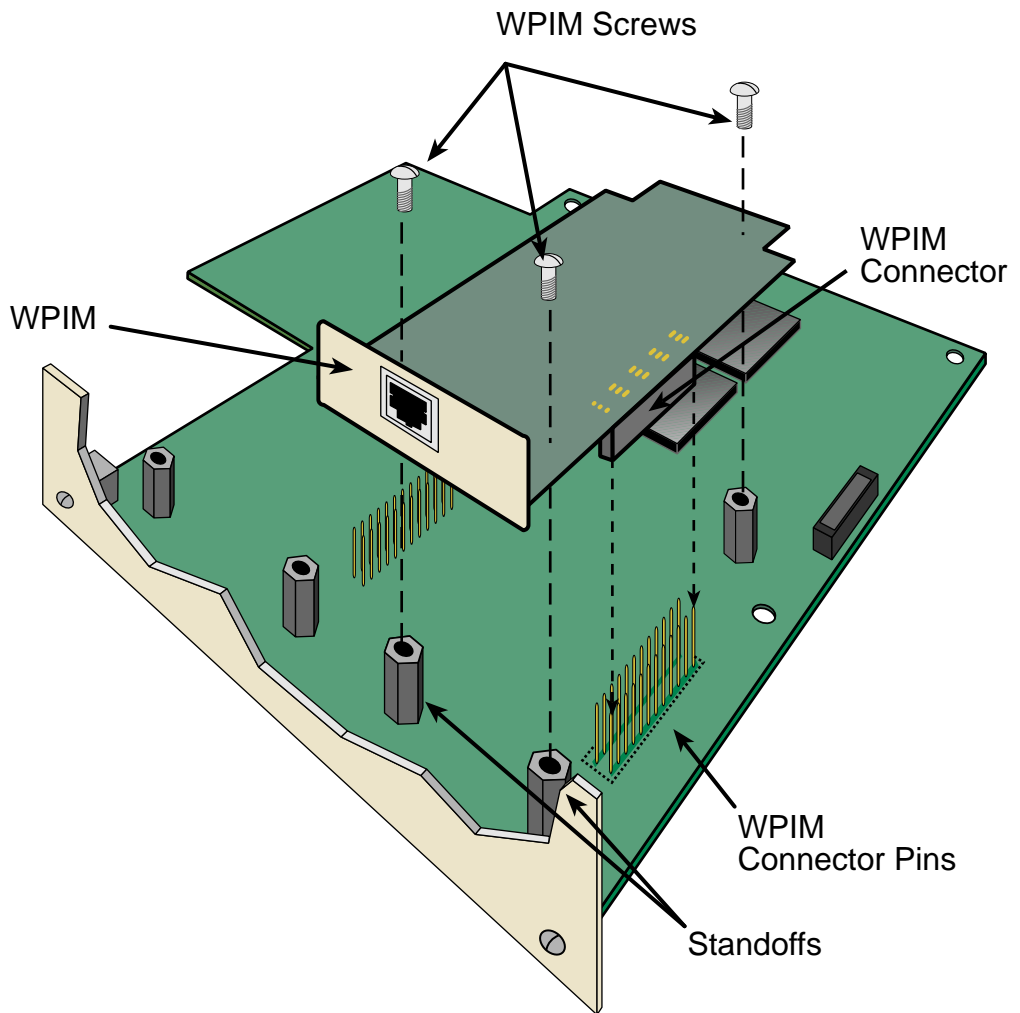
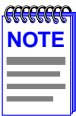


Figure 13 Installing WPIMs

CSX-COMP/ENCR Installation

This section contains instructions on how to install the CSX-COMP/ENCR into the CSX400 motherboard. To help eliminate any potential problems during or after installation, read and understand all of the following steps:

1. Attach one end of the antistatic wrist strap to your wrist and the other end to an approved electrical ground.
2. Unpack the CSX-COMP/ENCR by carefully removing it from the shipping box and then from the protective plastic bag. Do not cut the bag as the device could be damaged. If there are any signs of damage, contact the Cabletron Systems Global Call Center (refer to the [Getting Help](#) section).
3. Power down the CSX400 before you install the CSX-COMP/ENCR.
4. Remove the chassis cover of the CSX400 or CSX400-DC to install the CSX-COMP/ENCR (refer to [Removing the CSX400 Cover](#), on [page 58](#) or [Removing the CSX400-DC Cover](#), on [page 59](#)).



The motherboard of the CSX400 has two D-Type connectors. Use the left-most connector (as you are facing the front of the chassis). Ensure the CSX-COMP/ENCR is aligned such that its connector pins correctly align with the D-Type connector on the chassis or module.

5. Locate the D-Type connector and the standoffs on the CSX400 (refer to [Figure 14](#)).
6. The D-Type connector pins of the CSX-COMP/ENCR only fit one way onto the CSX400 D-Type connector. Lower the CSX-COMP/ENCR onto the standoffs and align the connector with the connector pins. Carefully insert the connector pins of the CSX-COMP/ENCR into the CSX400 connector.
7. Press down firmly on the CSX-COMP/ENCR until the pins fit all the way into the connector.
8. Secure the CSX-COMP/ENCR with the standoff screws supplied with the CSX-COMP/ENCR.

The CSX-COMP/ENCR installation is complete.

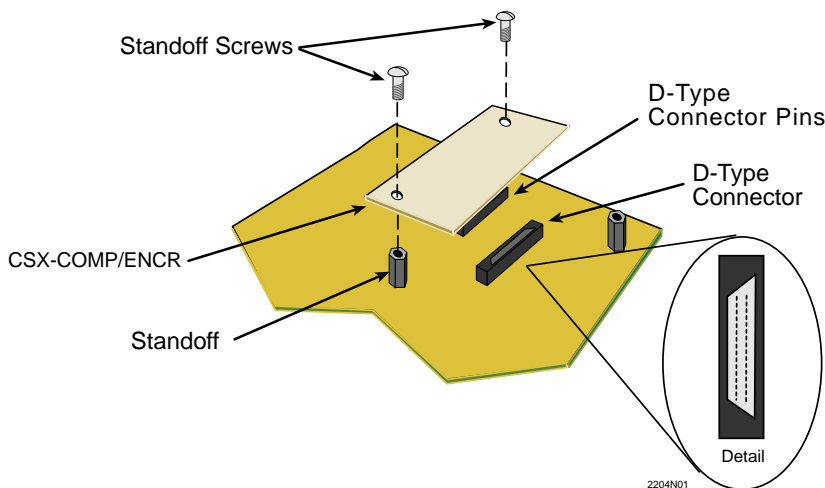


Figure 14 CSX-COMP/ENCR

Installing the CSX400

The CSX400 may be installed on a tabletop, shelf or in a 19-inch rack.

Refer to **Tabletop and Shelf Installations** for information concerning a tabletop or shelf installation. **CSX400 and CSX400-DC Rackmount Installation** describes the rackmount installation.

Tabletop and Shelf Installations

The following two subsections provide guidelines for installation on a tabletop or shelf.



Before performing installation procedures, ensure that the requirements outlined in the section, **Guidelines for Installations**, are met.

To install the CSX400 on a tabletop or shelf, locate the CSX400 within seven feet of its power source with an unrestricted free surface area as shown in **Figure 15**, and complete the following steps:

1. Locate the six round rubber feet included with your CSX400.

Installation

2. Peel the paper backing off the round rubber feet, and adhere them to the bottom of the CSX400. Place one rubber foot near each of the four corners of the CSX400, and evenly space the remaining two near the center.

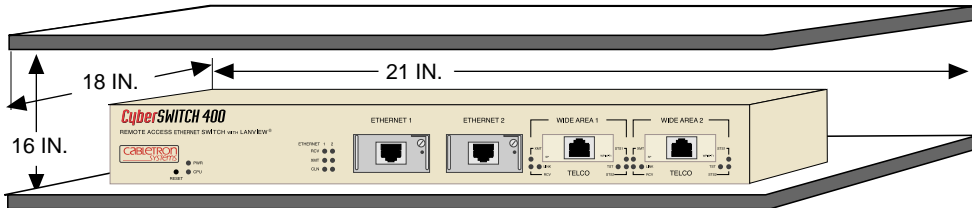


Figure 15 Tabletop or Shelf Installation

Continue the installation by connecting power as described in [Connecting the CSX400-DC to the Power Source](#).

CSX400 and CSX400-DC Rackmount Installation

There are two methods of attaching the rackmount brackets, included with the CSX400 and CSX400-DC, that are discussed in this section. [Attaching the Rackmount Brackets to the CSX400](#) discusses a typical installation of the CSX400, and [Bonding the Rackmount Brackets to the CSX400-DC](#) discusses the GR-1089-CORE Section 9 bonding requirements for the CSX400-DC when installing rackmount brackets. Refer to the procedure that applies to your installation.



Before installing the CSX400 or CSX400-DC into a rack, ensure that the rack supports the device(s) without compromising the stability of the rack. Otherwise, personal injury and/or equipment damage may result.

Rackmounting the CSX400 requires the following steps:

- Attaching the rackmount brackets
- Installing the CSX400 in a 19-inch rack
- Connecting the CSX400 to a power source

Tools Required

- Phillips screwdriver

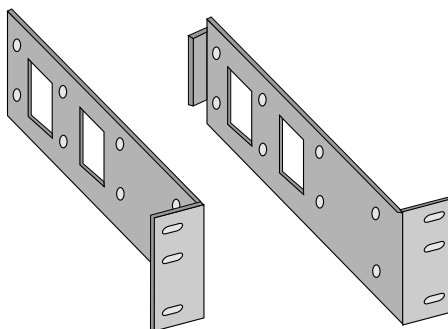
Materials Required

The following parts are included with the CSX400:

- Left (P/N 8501242-01) and right (P/N 8501241-01) rackmount brackets (**Figure 16**).
- 6-32 x 1/4 inch flat-head screws (4)



Do not use screws other than those supplied with the CSX400 to perform the following procedures.



Rackmount Brackets (2)

Figure 16 CSX400 and CSX400-DC Rackmount Hardware

Attaching the Rackmount Brackets to the CSX400

Refer to **Figure 17** and proceed as follows to attach the rackmount brackets:

1. Remove and save the four 6-32 x 1/4 inch flat-head screws that are located along the front edges of each side of the CSX400.
2. Locate the two rackmount brackets from the package included with your CSX400.

- Using the four 6-32 x 1/4 inch flat-head screws, attach the rackmount brackets to the sides of the CSX400 as shown in **Figure 17**.

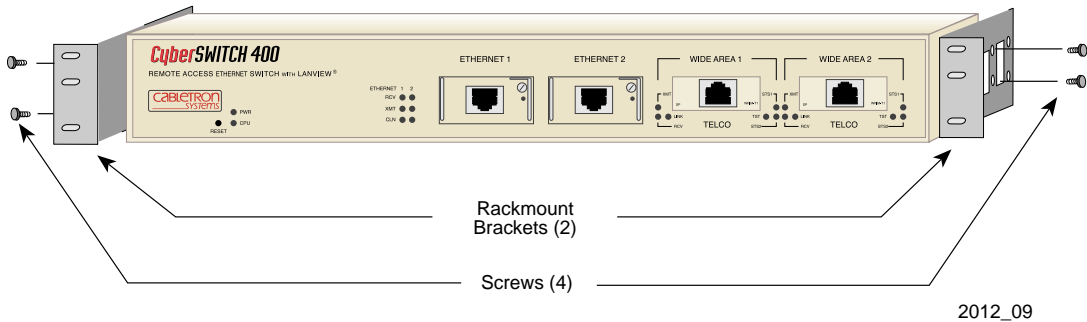


Figure 17 Installing the Rackmount Brackets

- Position the CSX400 between the vertical frame members of the 19-inch rack.
- Fasten the CSX400 with mounting screws as shown in **Figure 19**.

Bonding the Rackmount Brackets to the CSX400-DC

If the CSX400-DC is going to be mounted in a rack and needs to meet the GR-1089-CORE Section 9 bonding requirements, use the following instructions to install it into a 19-inch rack.

- Remove and discard the four cover screws (two from each side) located along the front edges of each side of the CSX400-DC.
- Remove the paint from around the area near the mounting holes on the left and right side of the cover of the CSX400-DC. See **Figure 18**.
- Apply a thin layer of anti-oxidant to the surface where the paint was removed.

4. Locate the four 6-32 x 3/8-inch flathead cover replacement screws in the rackmount kit. Use these screws to attach the rackmount brackets to the CSX400-DC as shown in **Figure 18**.

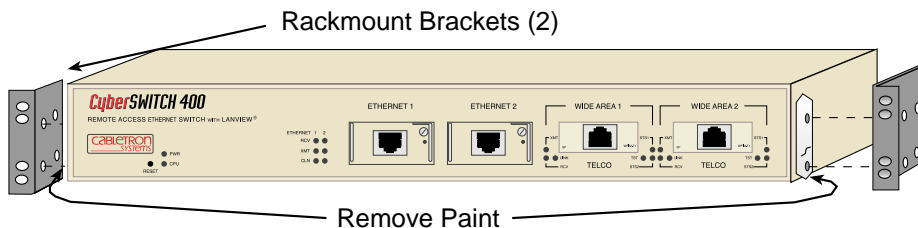


Figure 18 Installing the Rackmount Brackets

5. Position the CSX400 between the vertical frame members of the 19-inch rack.
6. Fasten the CSX400-DC with thread-forming screws as shown in **Figure 19**.

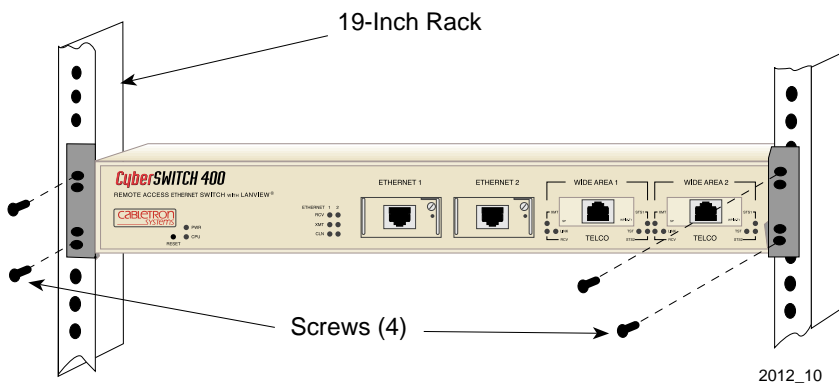
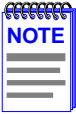


Figure 19 Installing the CSX400 and CSX400-DC in a Rack

Connecting the CSX400 to the Power Source



The CSX400 has a universal power supply. This allows you to connect the CSX400 to power sources of 100–125 and 200–240 Vac, 50/60 Hz.

To connect the CSX400 to the power source, perform the following steps:

1. Plug the power cord into the back panel of the CSX400.
2. Plug the other end of the power cord into a grounded wall outlet.
3. Verify that the **PWR** LED is on, indicating that the CSX400 is receiving power. After the CSX400 runs a self test, the **CPU** LED blinks green indicating normal operation. If the LED remains red, the processor is faulty; contact Cabletron Systems Technical Support (refer to **Getting Help** in **Chapter 1**.)
4. Proceed to **Chapter 7** to configure the CSX400.

Connecting the CSX400-DC to the Power Source

The CSX400-DC requires either a 48 Vdc or 60 Vdc (48/60 Vdc), 3.5 A (maximum), external power source supplied by three 18 AWG (American Wire Gauge) copper wires. These wires must be terminated to the dc input power strip shown in **Figure 20** with either ring or spade terminals. The dc power supply in the CSX400-DC has its own on/off switch and is rated at 100 watts. To connect the CSX400-DC to a 48/60 Vdc power source, face the back panel, then refer to **Figure 20** and proceed as follows:



ONLY QUALIFIED PERSONEL SHOULD PERFORM THESE INSTALLATION PROCEDURES.



TO REDUCE THE RISK OF ELECTRIC SHOCK OR ENERGY HAZARDS:

- CONNECT TO A RELIABLY GROUNDED 48/60 VDC SELV SOURCE.
- ENSURE THE BRANCH CIRCUIT OVERCURRENT PROTECTION IS RATED AT A MINIMUM OF 10 A.
- USE 18 AWG SOLID COPPER CONDUCTORS ONLY.
- ENSURE THAT A READILY ACCESSIBLE DISCONNECT DEVICE THAT IS SUITABLY APPROVED AND RATED, IS INCORPORATED IN THE FIELD WIRING.

TO BE INSTALLED IN A RESTRICTED ACCESS AREA IN ACCORDANCE WITH THE NEC OR THE AUTHORITY HAVING JURISDICTION.

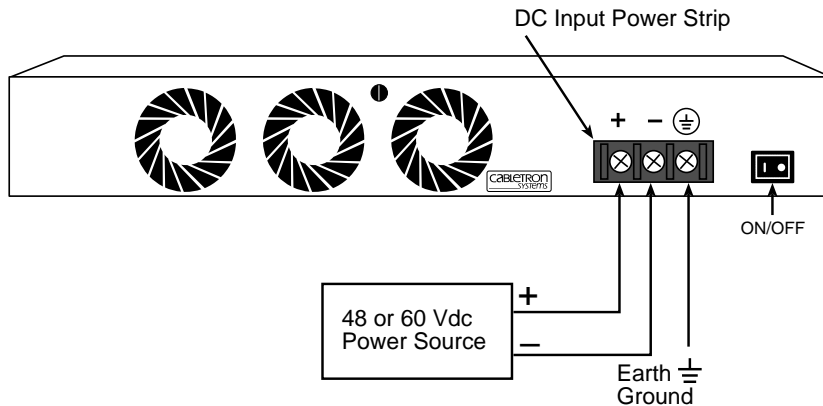


Figure 20 48/60 Vdc Power Supply Connections



To prevent injury or damage to the equipment, remove power from the 48/60 Vdc power source before proceeding with the following steps:

1. Connect the ground (⊕) terminal of the dc input power strip to an appropriate earth ground (green wire from power supply).
2. Refer to **Figure 20** for the proper connections to a 48/60 Vdc power source. Then connect the output leads of the 48/60 Vdc power source being used to the labeled negative (-) and positive (+) terminals on the dc input power strip.
3. Restore power to the 48/60 Vdc power sources.
4. Press the on/off power switch on.



The CSX400 sounds an audible alarm if there is a polarity reversal. If the alarm sounds, turn off the 48/60 Vdc power source to that power supply. Then reverse the positive and negative leads to the dc input power strip of that power supply. Restore power from the 48/60 Vdc power source. Press the on/off switch to on. If the alarm sounds again, press the power switch to off and call Cabletron Systems. Refer to **Getting Help**.

7

CSX400 Configuration with *QuickSET*

This chapter provides step-by-step instructions for configuring the CSX400 using *QuickSET*.



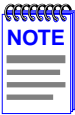
Before configuring the device, you must set up your computer based on the *READ ME FIRST!* documentation included with the product and installed the CSX400 using the *QuickSTART* Guide located in the *QuickSET* CD case.

Normally, *QuickSET* automatically establishes a communication link with the CSX400 being configured. However, under certain circumstances, *QuickSET* may not be able to locate the CSX400 automatically. In this case, the IP Address window shown in **Figure 21** displays:

A screenshot of a Windows-style dialog box titled "IP Address". The dialog box has a blue title bar with a red icon on the left and a close button (X) on the right. The main area is light gray and contains the text "Enter the IP Address and SuperUser Password of a QuickSET capable device." Below this text are two input fields. The first field is labeled "IP Address:" and contains the text "192.168.254.254". The second field is labeled "QuickSET Password:" and contains the text "xxxxxx". At the bottom of the dialog box are two buttons: "OK" and "Cancel".

Figure 21 IP Address Window

Enter the IP address of the CSX400 in the appropriate field and the password if applicable (the default password is *public*). Click on the **OK** button and *QuickSET* locates the CSX400 on the network and displays the First Introductory window shown in **Figure 22**.



The *QuickSET* version number shown on each window in this chapter may not reflect the *QuickSET* version number running on your system.



Figure 22 First Introductory Window

Click on the **Next>>** button to continue the CSX400 configuration, and the Second Introductory window shown in **Figure 23** displays.

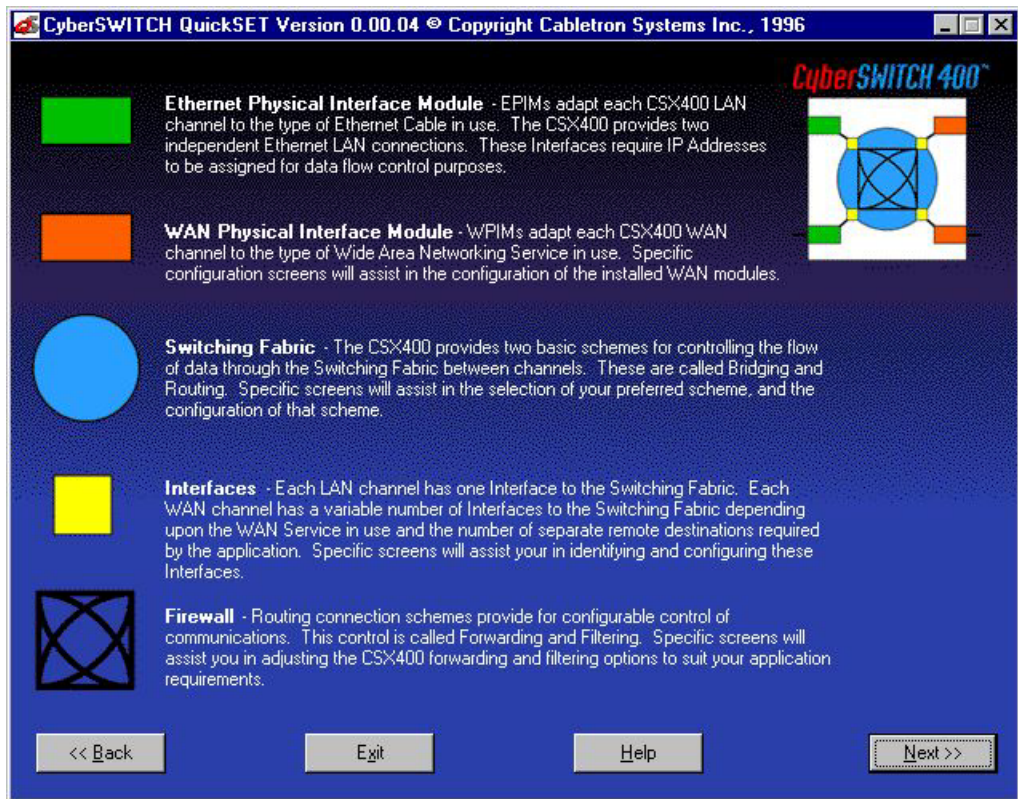


Figure 23 The Second Introductory Window

Click on the **Next>>** button and go to the Ethernet 1 and 2 configuration window to continue the CSX400 configuration.

Ethernet Configuration

This section explains how to configure the CSX400 Ethernet 1 and 2 fields using *QuickSET*.

Ethernet 1 and 2 Configuration Window

The Ethernet 1 and 2 configuration window, shown in **Figure 24**, displays after clicking on the **Next>>** button in the Second Introductory window. The Local Ethernet IP address and Subnet Mask fields shown on the Ethernet 1 and 2 configuration window are used for setting an IP address and Subnet Mask.

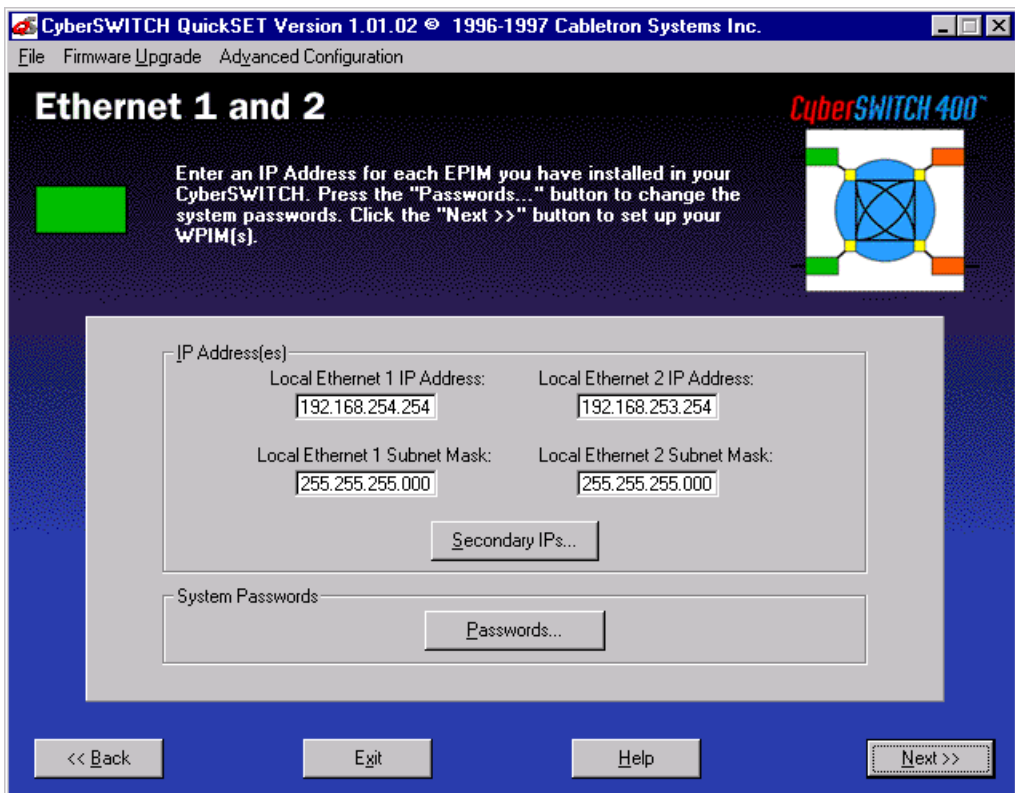


Figure 24 Ethernet 1 and 2 Configuration Window

This section describes each of the fields on the Ethernet 1 and 2 configuration window.

Local Ethernet 1 IP Address — Displays the IP address for Ethernet interface 1. Place the cursor in this field and type the preferred IP address in Dotted Decimal Notation (DDN) format. The IP address must be entered in this field to continue.

Local Ethernet 1 Subnet Mask — The Subnet Mask takes the same form as an IP address; four groups of three decimal digits, separated by periods. Each group must be in the numerical range of 0 to 255. The first time you use *QuickSET*, the Subnet Mask field displays a default Subnet Mask, based on the IP address entered, when it is clicked on. If you wish to use a different Subnet Mask, enter it at this time in DDN format. A Subnet Mask must be entered in this field to continue.

Local Ethernet 2 IP Address — Displays the IP address for Ethernet interface 2. Place the cursor in this field and type in the preferred IP address in DDN format.

Local Ethernet 2 Subnet Mask — Displays the Subnet Mask for Ethernet interface 2. Place the cursor in this field and type in the Subnet Mask in DDN format. The first time you use *QuickSET*, the Subnet Mask field displays a default Subnet Mask, based on the IP address entered, when it is clicked on. If you wish to use a different Subnet Mask, enter it at this time, and type the Subnet Mask in DDN format. A Subnet Mask must be entered in this field to continue if an IP address is entered for the Local Ethernet 2 interface.

Secondary IPs — The Secondary IPs window shown in **Figure 25** displays after clicking on the **Secondary IPs...** button, and shows the list of current Secondary IP addresses. The CSX400 can support multiple IP Subnets, therefore, there can be multiple Secondary IP Addresses assigned to an Ethernet interface. To add a Secondary IP address, click on the **Add IP** button and enter the IP Address, and Subnet Mask in their corresponding fields.

When you have finished making changes, click on the **Apply Changes** button. Click on the **Done** button when you are finished.

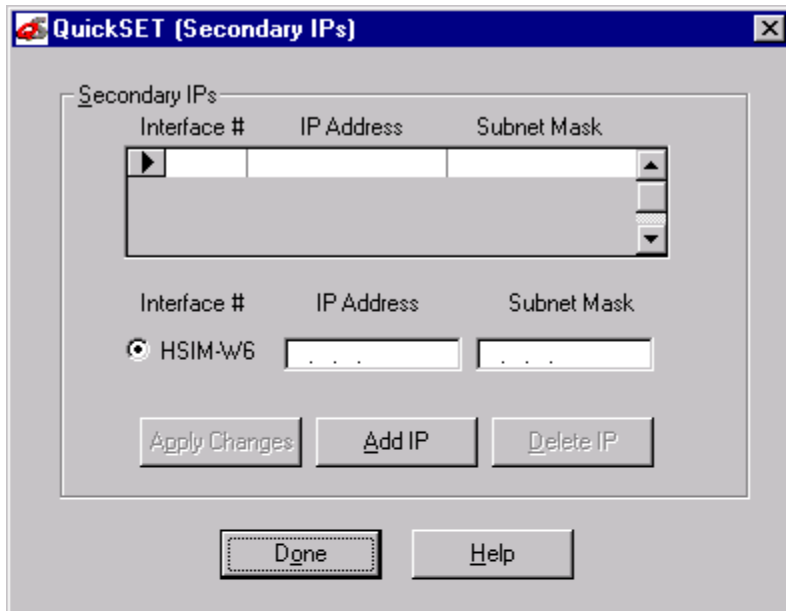



Figure 25 Secondary IPs Window

System Passwords — The System Passwords window shown in **Figure 26** displays after clicking on the **Passwords** button in the Ethernet 1 and 2 configuration window. The system passwords used by *QuickSET* are the same as the Community Names of the device that are used in Local Management through a TELNET application. System passwords allow you to control management access by establishing three passwords. Each password controls varying levels of access to the CSX400 management.

Once passwords are assigned, you must use the SuperUser System password at the User Password prompt when initiating a *QuickSET* session. If you are configuring the CSX400 for the first time or if no passwords are assigned, the default System password for each access level is preset to *public*.



The image shows a Windows-style dialog box titled "CyberSWITCH System Passwords". The title bar is blue with a small icon on the left and a close button (X) on the right. The main area has a light gray background. At the top, it says "Enter the passwords that you want enforced when accessing this CyberSWITCH." Below this, there are three sets of password fields. Each set consists of a label followed by two text input boxes. The first set is for "Read Only Access", the second for "Read/Write Access", and the third for "QuickSET (SuperUser)". Each label has a small icon to its left. At the bottom, there are two buttons: "OK" and "Cancel". Below the input fields, there is a note: "Note: You must save your configuration before these passwords will be in effect. All passwords will be converted to lower case. Blank passwords will be converted to 'public'."

CyberSWITCH System Passwords

Enter the passwords that you want enforced when accessing this CyberSWITCH.

Read Only Access:

Confirm Password:

Read/Write Access:

Confirm Password:

QuickSET (SuperUser):

Confirm Password:

Note: You must save your configuration before these passwords will be in effect. All passwords will be converted to lower case. Blank passwords will be converted to "public".

OK Cancel

Figure 26 System Passwords Window

The following definitions explain the fields in the System Passwords window shown in **Figure 26**.

Read Only Access — This access level allows reading of device parameters not including system passwords. Place the cursor in this field and type the new system password. Retype the system password in the Confirm Password field below the Read Only Access field.

Read/Write Access — This access level allows editing of some device configuration parameters not including changing system passwords. Place the cursor in this field and type the new system password. Retype the system password in the Confirm Password field below the Read/Write Access field.

QuickSET (SuperUser) — This access level allows full management privileges. Place the cursor in this field and type the new system password. Retype the system password in the Confirm Password field below the *QuickSET* (SuperUser) field.

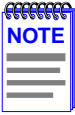


If you edit the SuperUser system password, be certain not to forget it. If you do, you cannot perform management functions without returning the device to its factory default configuration. This effectively erases any configuration work you may have done.

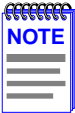
When finished configuring the CSX400 system passwords, click on the **OK** button in the System Passwords window to return to the Ethernet 1 and 2 configuration window.

Once your Ethernet configuration is complete, click on the **Next>>** button and go to the **Wide Area 1 and 2 Configuration** section.

Wide Area 1 and 2 Configuration



When configuring WAN interfaces 1 and 2 with *QuickSET*, the Wide Area configuration window that displays corresponds to the specific WPIM that is installed into the CSX400.



Configuration for the Wide Area 2 interface is the same as the configuration for the Wide Area 1 interface.

Both Wide Area 1 and Wide Area 2 slots must be populated to initiate Wide Area interface 2 configuration.

Refer to the appropriate section listed below to configure your Wide Area 1 or 2 interface on the CSX400:

Wide Area T1 Configuration Window

Wide Area E1 Configuration Window

Wide Area DI Configuration Window

Wide Area Synchronous Configuration Window

Wide Area DDS Configuration Window

Wide Area HDSL Configuration Window

Wide Area T1 Configuration Window

The Wide Area T1 configuration window shown in **Figure 27** displays after clicking on the **Next>>** button in either the Ethernet 1 and 2 configuration window or the Wide Area Frame Relay Time Slot and PPP configuration windows, depending on whether you have installed one or two WPIMs in the CSX400, and in what order you are configuring them.

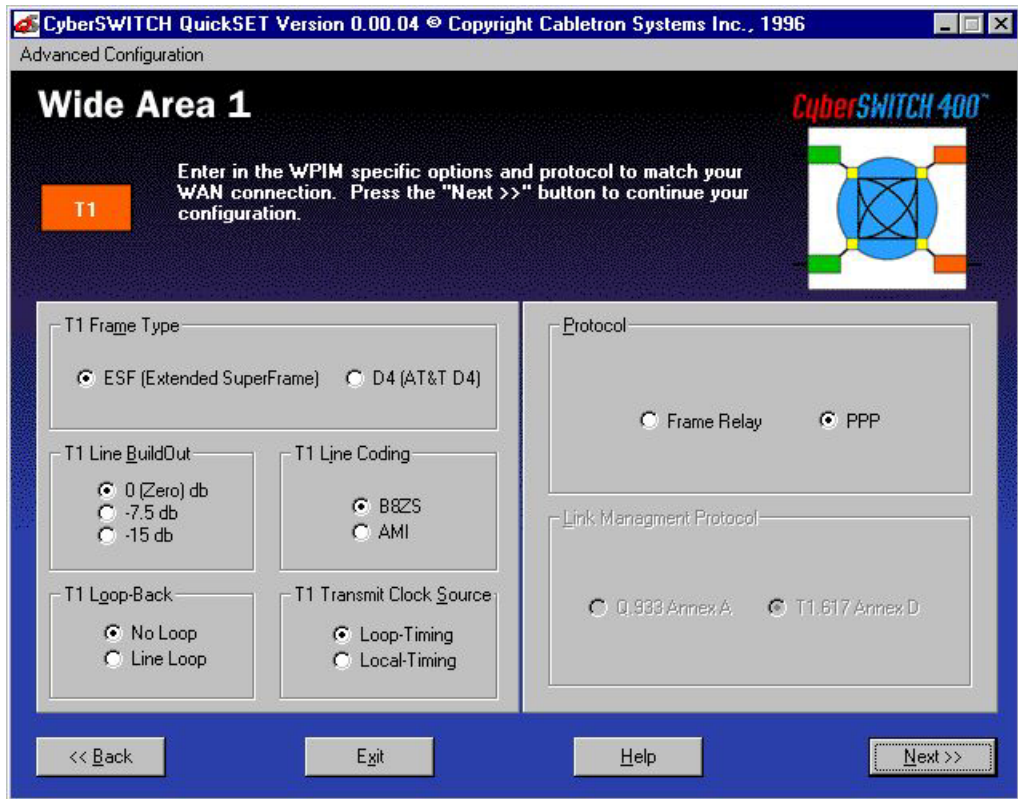
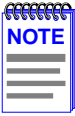


Figure 27 Wide Area T1 Configuration Window

This section explains how to configure the CSX400 Wide Area T1 interface using *QuickSET*.



The service provider (i.e., AT&T, Sprint, MCI, etc.) determines the settings for many of the following fields. Consult the service provider for the correct settings.

The line configuration information shown in **Table 12** must be supplied by your service provider. The CSX400 factory default settings are in bold.

Table 12 Telco Configuration Information

Configuration Information Required by User	Configuration Information Supplied by Service Provider
T1 Frame Type	ESF or D4
T1 Line BuildOut	0 dB , -7.5 dB, -15 dB
T1 Line Coding	B8ZS or AMI
T1 Loop-Back	No Loop or Line Loop
T1 Transmit Clock Source	Loop-Timing or Local-Timing
Time Slots (for Fractional T1)	Time Slot (1-24) Assignments

The following definitions explain the fields in the T1 WAN configuration window.

T1 Frame Type — Displays the T1 frame type. The selections are ESF (Extended Superframe) and D4 (AT&T D4). The default setting for this field is **ESF**.

T1 Line BuildOut — Displays the signal level for the physical T1 line. Set this to 0 dB unless the service provider recommends another setting. The default setting for this field is **0 dB**. The following options are available for this setting:

- 0 dB
- -7.5 dB
- -15 dB

T1 Line Coding — Displays the line coding for the physical T1 line. The selections for this field are B8ZS and AMI. The default setting for this field is **B8ZS**.

T1 Loop-Back — Network Loopback is a testing procedure that segments the line and allows you to isolate faults. The selections for this field are No Loop and Line Loop. In Line Loop all 24 channels are looped back to the T1 line. The CyberSWITCH must be in Loop-Timing mode to use this option. The default setting is **No Loop**.

T1 Transmit Clock Source — Displays the T1 Transmit Clock Source. The choices for this field are Loop-Timing (Extracted Line Data) and Local-Timing (Internal Clock). The default setting for this field is **Loop-Timing**.

Protocol — Displays the active protocol for the Wide Area T1 interface. The selections for this field are either Frame Relay or Point-to-Point (PPP). The default setting for this field is **PPP**.

Link Management Protocol — If Frame Relay is the selected protocol, this field displays Q.933 Annex A and T1.617 Annex D. The default for Frame Relay is **T1.617 Annex D**. This field is grayed out and not used for PPP.

Once the Wide Area T1 configuration is complete, click on **Next>>**, and go to the **Wide Area Frame Relay Time Slot Configuration Window** or **Wide Area PPP Time Slot Configuration Window** section, depending on which protocol you are using.

Wide Area E1 Configuration Window

The Wide Area (E1) configuration window shown in **Figure 28** displays after clicking on the **Next>>** button in either the Ethernet 1 and 2 configuration window or the Wide Area Frame Relay Time Slot and PPP configuration windows, depending on whether you have installed one or two WPIMs in the CSX400, and what order you are configuring them.

This section explains how to configure the CSX400 E1 WAN interface using *QuickSET*.

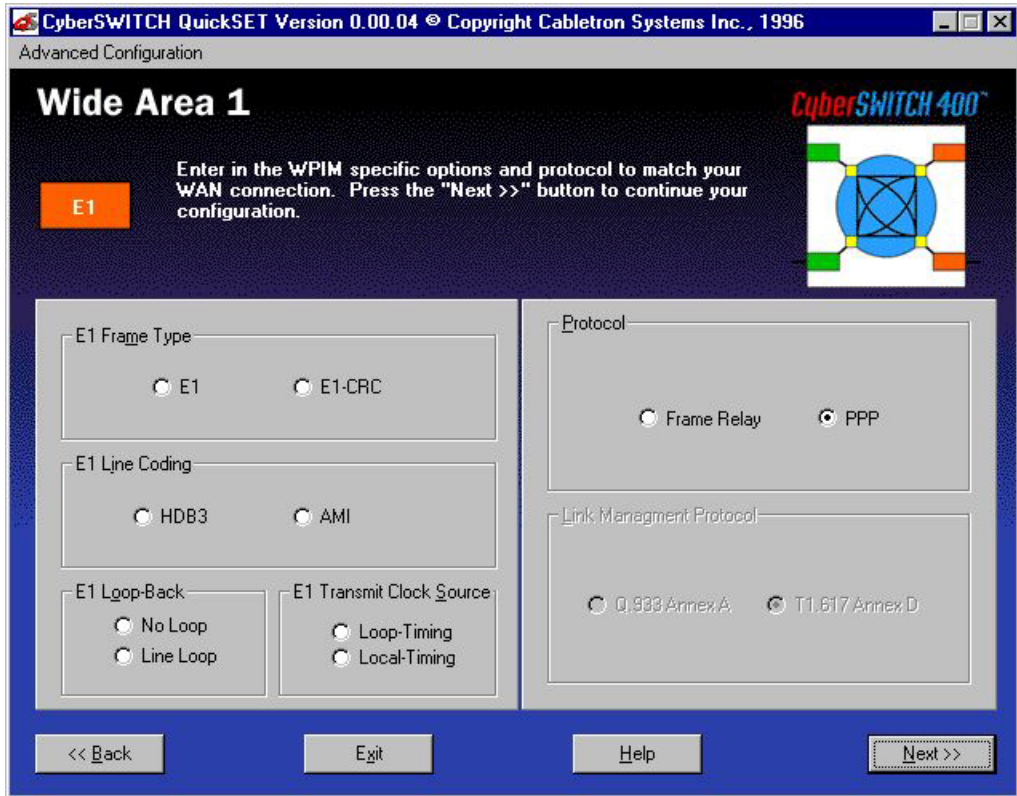


Figure 28 Wide Area E1 Configuration Window



The service provider determines the settings for the following fields. Consult the service provider for the correct settings.

The line configuration information shown in **Table 13** must be supplied by your service provider. The CyberSWITCH factory default settings are in **bold** type.

Table 13 Telco Configuration Information

Configuration Information Required by User	Configuration Information Supplied by Service Provider
E1 Frame Type	E1 or E1-CRC
E1 Line Coding	HDB3 or AMI
E1 Loop-Back	No Loop or Line Loop
E1 Transmit Clock Source	Loop-Timing or Local-Timing
Time Slots (for Fractional E1)	Time Slot (1-32) Assignments

The following definitions explain the fields in the Wide Area E1 configuration window.

E1 Frame Type — Displays the E1 frame type. The selection toggles between E1 and E1-CRC. The default setting for this field is **E1**.

E1 Line Coding — Displays the line coding for the physical E1 line. The selections toggle between HDB3 and AMI. The default setting for this field is **HDB3**.

E1 Loop-Back — Network Loopback is a testing procedure that segments the line and allows you to isolate faults. Click on the radio button to select either the **No Loop** or **Line Loop** option. In Line Loop, all 32 channels are looped back to the E1 line. The CyberSWITCH must be in Loop-Timing mode to use this option. The default setting is **No Loop**.

E1 Transmit Clock Source — Displays the E1 Transmit Clock Source. Click on the radio button to select either the **Loop-Timing** (Extracted Line Data) or **Local-Timing** (Internal Clock) option. The default setting for this field is **Loop-Timing**.

Protocol — Displays the active protocol for the E1 WAN port. The selections for this field are either **Frame Relay** or **PPP**. The default setting for this field is **PPP**.

Link Management Protocol — If Frame Relay is the selected protocol, this field displays Q.933 Annex A and T1.617 Annex D. The default for Frame Relay is **T1.617 Annex D**. This field is grayed out and not used for PPP.

Once the E1 WAN configuration is complete, click on the **Next>>** button and go to the **Wide Area Frame Relay Time Slot Configuration Window** or **Wide Area PPP Time Slot Configuration Window** section, depending on which protocol you are using.

Wide Area DI Configuration Window

The Wide Area (DI) configuration window shown in **Figure 29** displays after clicking on the **Next>>** button in the Ethernet 1 and 2 configuration window or the Wide Area Frame Relay Time Slot and PPP configuration windows, depending on whether you have installed one or two WPIMs in the CSX400, and in what order you are configuring them.

This section explains how to configure the CSX400 Wide Area DI interface using *QuickSET*.



Figure 29 Wide Area DI Configuration Window



The service provider (i.e., AT&T, Sprint, MCI, etc.) determines the settings for the following fields. Consult the service provider for the correct settings.

The line configuration information shown in **Table 14** must be supplied by your service provider. The CyberSWITCH factory default settings are in bold.

Table 14 Telco Configuration Information

Configuration Information Required by User	Configuration Information Supplied by Service Provider
T1 Frame Type	ESF or D4
T1 Line BuildOut	0dB , -7.5 dB, -15 dB
T1 Line Coding	B8ZS or AMI
T1 Loop-Back	No Loop or Line Loop
T1 Transmit Clock Source	Loop-Timing or Local-Timing
Time Slots (for Fractional T1)	Time Slot (1-24) Assignments

The WPIM-DI has two connectors allowing two devices to share the available Time Slots in a T1 WAN link. The Network Interface (NI) is the main connection to the WAN link while the Drop-and-Insert (DI) interface is used by other T1 equipment to share the main T1 link.

The following definitions explain the fields in the DI WAN configuration window.

DI Functionality — Displays the status of the Drop-and-Insert function. Click on the **Enable** radio button to enable the Drop-and-Insert function, that allows any Time Slots set to 0 in the Wide Area Frame Relay Time Slot and PPP configuration windows to be used by the Drop-and-Insert port interface.

T1 Frame Type — Displays the DI frame type. Click on the radio button to select either the ESF or D4 option. The default setting for this field is **ESF**.

T1 Line BuildOut — Displays the signal level for the physical DI line. Set this to 0 dB unless the service provider recommends another setting. The default setting for this field is **0 dB**. Click on the appropriate radio button for the following levels:

- 0 (Zero) dB
- -7.5 dB
- -15 dB

T1 Line Coding — Displays the line coding for the physical DI line. The selections toggle between B8ZS and AMI. The default setting for this field is **B8ZS**.

T1 Loop-Back — Network Loopback is a testing procedure that segments the line and allows you to isolate faults. The selections for this field toggle between No Loop and Line Loop. In Line Loop all 24 channels are looped back to the DI line. The CyberSWITCH must be in Loop-Timing mode to use this option. The default setting is **No Loop**.

T1 Transmit Clock Source — Displays the DI Transmit Clock Source. Click on the radio button to select either the **Loop-Timing** (Extracted Line Data) or **Local-Timing** (Internal Clock) option. The default setting for this field is **Loop-Timing**.

Protocol — Displays the active protocol for the Wide Area DI interface. The selections for this field are **Frame Relay** and **PPP**. The default setting for this field is **PPP**.

Link Management Protocol — If Frame Relay is the selected protocol, this field displays Q.933 Annex A and T1.617 Annex D. The default for Frame Relay is **T1.617 Annex D**. This field is grayed out and not used for PPP.

Once the Wide Area DI configuration is complete, click on the **Next>>** button, and go to the **Wide Area Frame Relay Time Slot Configuration Window** or the **Wide Area PPP Time Slot Configuration Window** section, depending on which protocol you are using.

Wide Area Synchronous Configuration Window

The Wide Area Synchronous configuration window shown in **Figure 30** displays after clicking on the **Next>>** button in either the Ethernet 1 and 2 configuration window or the Wide Area Frame Relay Time Slot and PPP configuration windows, depending on whether you have installed one or two WPIMs in the CSX400, and in what order you are configuring them.

This section explains how to configure the CSX400 Synchronous WAN port using *QuickSET*.

CyberSWITCH 400 QuickSET Version 1.01.03 © 1996-1997 Cabletron Systems Inc.

File Firmware Upgrade Advanced Configuration

Wide Area 1

SYNC Enter in the WPIM specific options and protocol to match your WAN connection. Press the "Next >>" button to continue your configuration.

Sync Port Type

- ☒ V.35
- ☐ RS232
- ☐ RS422
- ☐ X.21

Sync Clock Speed

64000

Sync Flow Control

- ☐ Force CTS True
- ☐ Force DSR True

Protocol

- ☐ Frame Relay
- ☒ PPP

Link Management Protocol

- ☐ Q.933 Annex A
- ☒ T1.617 Annex D

<< Back Exit Help Next >>

Figure 30 Wide Area Synchronous Configuration Window



The service provider (i.e., AT&T, Sprint, MCI, etc.) determines the settings for the following fields. Consult the service provider for the correct settings.

The line configuration information shown in **Table 15** is determined by your service provider. The CSX400 factory default settings are in bold.

Table 15 Telco Configuration Information

Configuration Information Required by User	Configuration Information Supplied by Service Provider
Sync Port Type	V.35 , RS422, RS232 or X.21
Sync Flow Control	Force CTS on or off
	Force DSR on or off
Sync Clock Speed	64000

The following definitions explain the fields in the Synchronous WAN configuration window.

Sync Port Type — Displays the Synchronous port electrical interface type. The selections for this field are V.35, RS422, RS232, and X.21. The default setting for this field is **V.35**. **Table 16** explains the options for the Sync Port Type.

Table 16 Sync Port Types

Sync Port Type	Interface Type	Cable Type	Cabletron Part Number
RS422	RS449	RS449	9380120
RS232	RS232	RS232	9380122
V.35	V.35	V.35	9380121
X.21	X.21	X.21	9380123
RS422	RS530	RS530	9380124
RS422	RS530A	RS530A	9380126
RS422	RS530 Alt A	RS530 Alt A	9380125
RS422	RS530A Alt A	RS530A Alt A	9380127

Sync Clock Speed — Displays your configured receive clock speed. The default setting for this field is **64000** bits per second. The information necessary for you to set this field is normally determined by the service provider. Select the down arrow button to make your selection from the list of clock speeds using the information provided by your service provider (if it is not listed, type the value in).

Sync Flow Control — Displays the source of the Clear To Send (CTS) and the Force Data Set Ready (DSR) signals.

The CTS signal is an input to the CSX400. The CSX400 can either use or ignore the CTS signal. Clicking on the box indicates that the CSX400 ignores the CTS signal from an external DCE (Data Communications Equipment) and forces the signal high. The off setting indicates that the CTS signal is received from an external DCE. The default setting is **off**.

The DSR signal is an input to the CSX400. Clicking on the box indicates that DSR signal is internally forced high. The off setting indicates that the DSR signal is received from an external DCE. The default setting is **off**.

Protocol — Displays the active protocol for the Wide Area Sync port. The selections for this field are either **Frame Relay** and **PPP**. The default setting for this field is **PPP**.

Link Management Protocol — If Frame Relay is the selected protocol, this field displays Q.933 Annex A and T1.617 Annex D. The default for Frame Relay is **T1.617 Annex D**. This field is grayed out and not used for PPP.

Once the Wide Area Synchronous configuration is complete, click on the **Next>>** button, and go to the **Bridging and Routing Configuration** section of this guide.

Wide Area DDS Configuration Window

The Wide Area DDS configuration window shown in **Figure 31** displays after clicking on the **Next>>** button in the Ethernet 1 and 2 configuration window or the Wide Area Frame Relay Time Slot and PPP configuration windows, depending on whether you have installed one or two WPIMs in the CSX400, and the order in which you are configuring them.

This section explains how to configure the CSX400 Wide Area DDS interface using *QuickSET*.

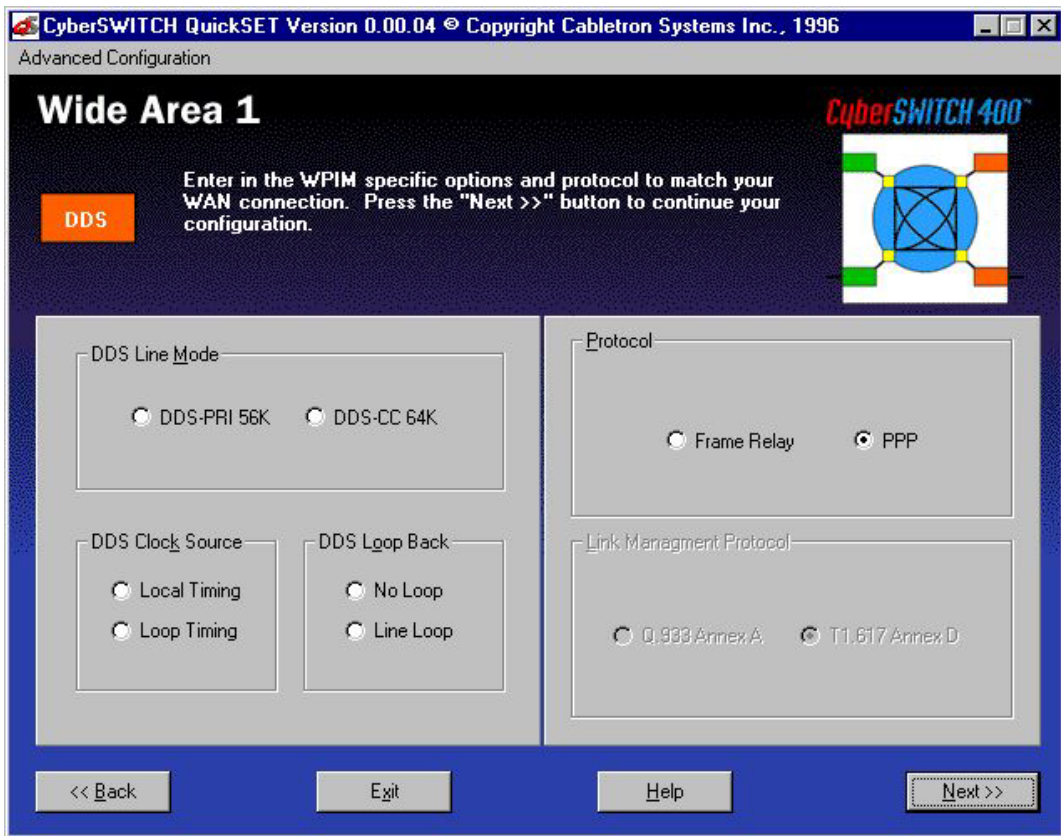


Figure 31 Wide Area DDS Configuration Window



The service provider (i.e., AT&T, Sprint, MCI, etc.) determines the settings for **Table 17**. Consult the service provider for the correct settings.

Table 17 shows the line configuration information normally determined by your service provider. The CSX400 factory default settings are in bold.

Table 17 Telco Configuration Information

Configuration Information Required by User	Configuration Information Supplied by Service Provider
DDS Line Mode	DDS-PRI or DDS-CC
DDS Clock Source	Loop-Timing or Local-Timing
DDS Loop Back	No Loop or Line Loop

This section describes the fields in the Wide Area DDS configuration window.

DDS Line Mode — Displays the DDS Line Mode. The selections for this field are DDS-PRI 56K (primary) and DDS-CC 64K (clear channel). This information is determined by the service provider. The default setting is **DDS-PRI**.

DDS Clock Source — Displays the DDS clock source. The selections for this field are either Loop-Timing or Local-Timing. The Loop-Timing setting allows the CSX400 to receive its timing information from the service provider. The Local-Timing setting allows the CSX400 to generate its timing information internally. If DDS-CC 64K was chosen for the DDS Line Mode then this field must be set to Loop-Timing. The default setting for this field is **Loop-Timing**.

DDS Loop Back — Displays the internal loopback as either Line Loop or No Loop. Line Loop is reserved for network diagnostics only. The default setting is **No Loop**.

Protocol — Displays the active protocol for the DDS WAN port. The selections for this field are **Frame Relay** or **PPP**. The default setting for this field is **PPP**.

Link Management Protocol — If Frame Relay is the selected protocol, this field displays Q.933 Annex A and T1.617 Annex D. The default for Frame Relay is **T1.617 Annex D**. This field is grayed out and not used for PPP.

Once the Wide Area DDS configuration is complete, click on the **Next>>** button, and go to the **Bridging and Routing Configuration** section of this guide

Wide Area HDSL Configuration Window

The Wide Area HDSL configuration window shown in **Figure 32** displays after clicking on the **Next>>** button in the Ethernet 1 and 2 configuration window or the PPP-HDSL configuration window.

This section explains how to configure the CSX400 Wide Area HDSL interface using *QuickSET*.

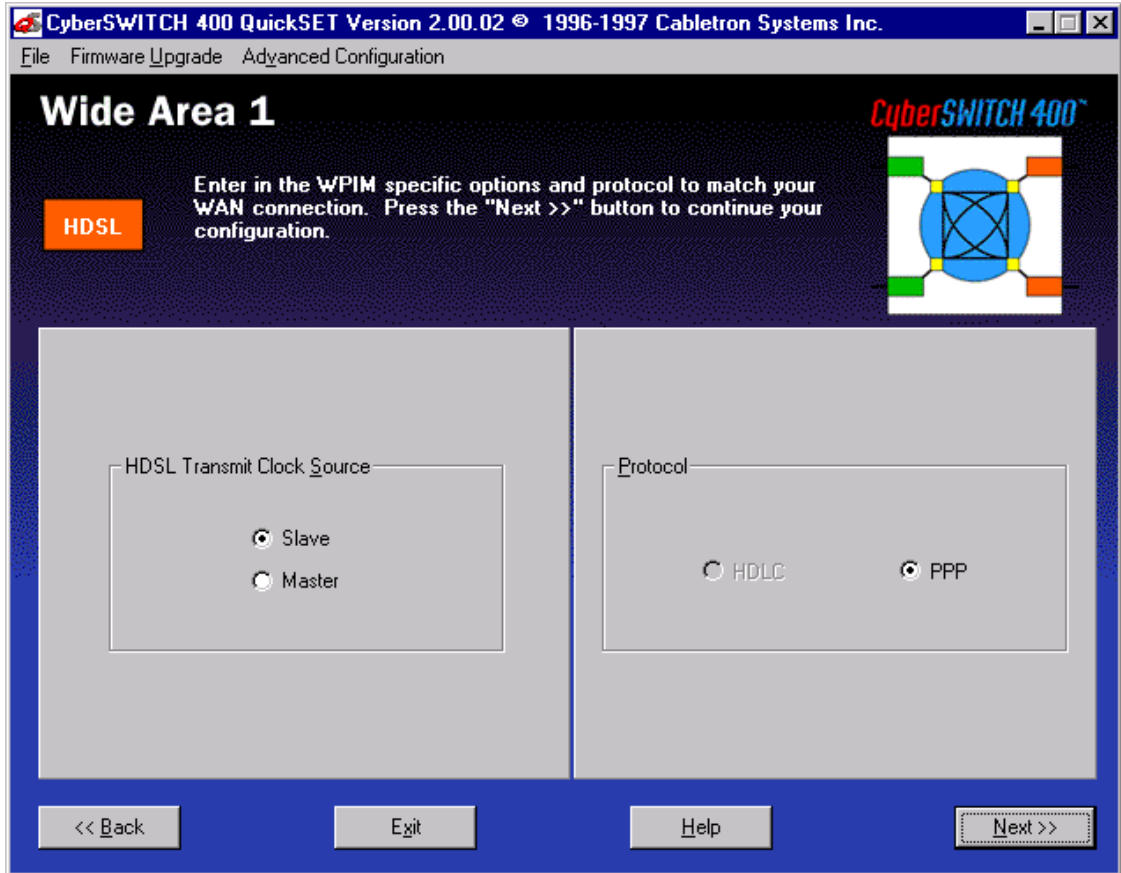


Figure 32 Wide Area HDSL Configuration Window



The wiring provider (i.e., Internet Service Provider (ISP) contractor, etc.) determines the settings for **Table 18**. Consult the service provider for the correct settings.

Table 18 shows the line configuration information normally determined by your wiring provider. The CSX400 factory default setting is in bold.

Table 18 Telco Configuration Information

Configuration Information Required by User	Configuration Information Supplied by Service Provider
HDSL Transmit Clock Source	Slave or Master

This section describes the fields in the Wide Area HDSL configuration window.

HDSL Transmit Clock Source — Displays the HDSL Transmit Clock Source. Click on the radio button to select either the Slave or Master option. The default setting is **Slave**.

Protocol — Displays the active protocol for the HDSL WAN port. The selections for this field are either HDLC or Point-to-Point (PPP). The default setting for this field is PPP.

Once the Wide Area HDSL configuration is complete, click on the **Next>>** button, and go to the **Wide Area HDSL Time Slot Configuration Window** section.

Wide Area Frame Relay Time Slot Configuration Window

The Wide Area Frame Relay Time Slot configuration window shown in **Figure 33** displays when you click on the **Next>>** button in the Wide Area T1, E1, or DI configuration windows when Frame Relay is chosen as the WAN Protocol.

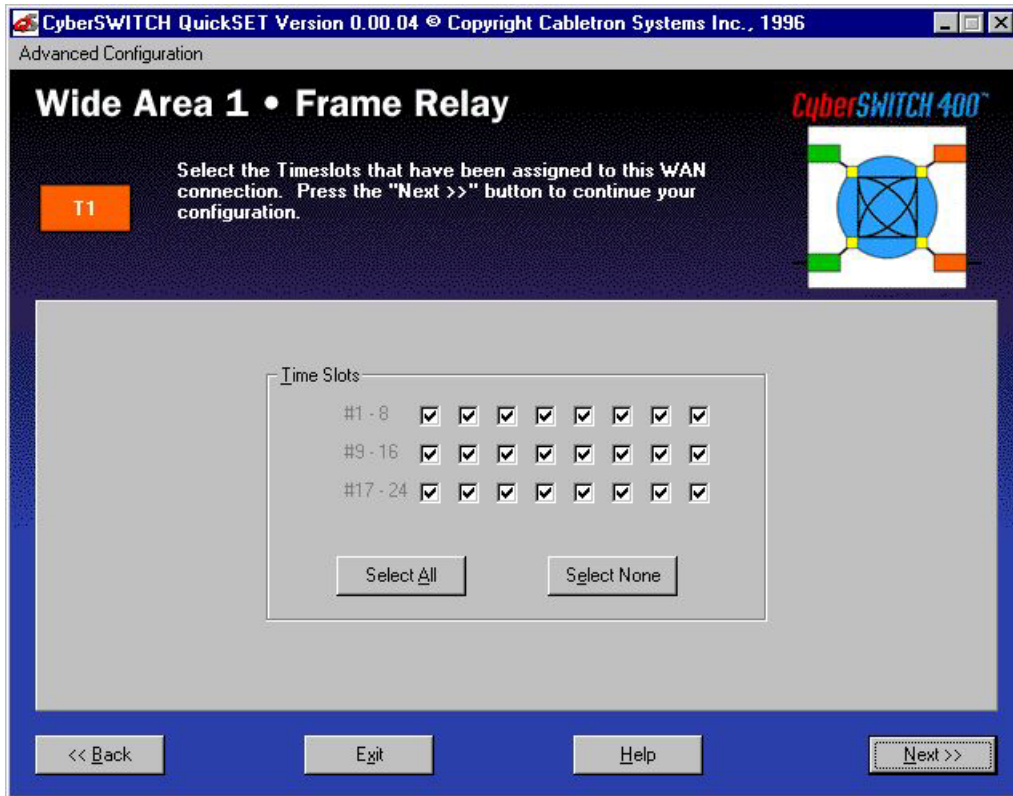
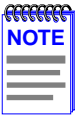


Figure 33 Wide Area Frame Relay Time Slot Configuration Window

The following section defines the fields in the Wide Area Frame Relay Time Slot configuration window.

Time Slots — A full line consists of 24 Time Slots (T1 and DI) or 31 Time Slots (E1), each capable of up to 64 Kbps throughput. If you are leasing an entire line from your service provider, you may select all the Time Slots by clicking the **Select All** button. A “check mark” displays in the selected box. If you have leased a portion of a fractional T1 or E1 line, the service provider tells you which Time Slots are allocated for your use. In this case, select only those Time Slots.



If you are configuring a WPIM-DI Time Slot table, any available Time Slots that are not checked are mapped to the DI Interface. In other words, If you lease an entire T1 line, any Time Slots that are not selected in the Frame Relay configuration window are used by the device connected to the DI interface.

Once the Wide Area Frame Relay Time Slot configuration is complete, click on the **Next>>** button, and go to the **Bridging and Routing Configuration** section.

Wide Area PPP Time Slot Configuration Window

The Wide Area PPP Time Slot configuration window shown in **Figure 34** displays when you click on the **Next>>** button in the Wide Area T1, E1, and DI configuration windows when PPP is chosen as the WAN Protocol.

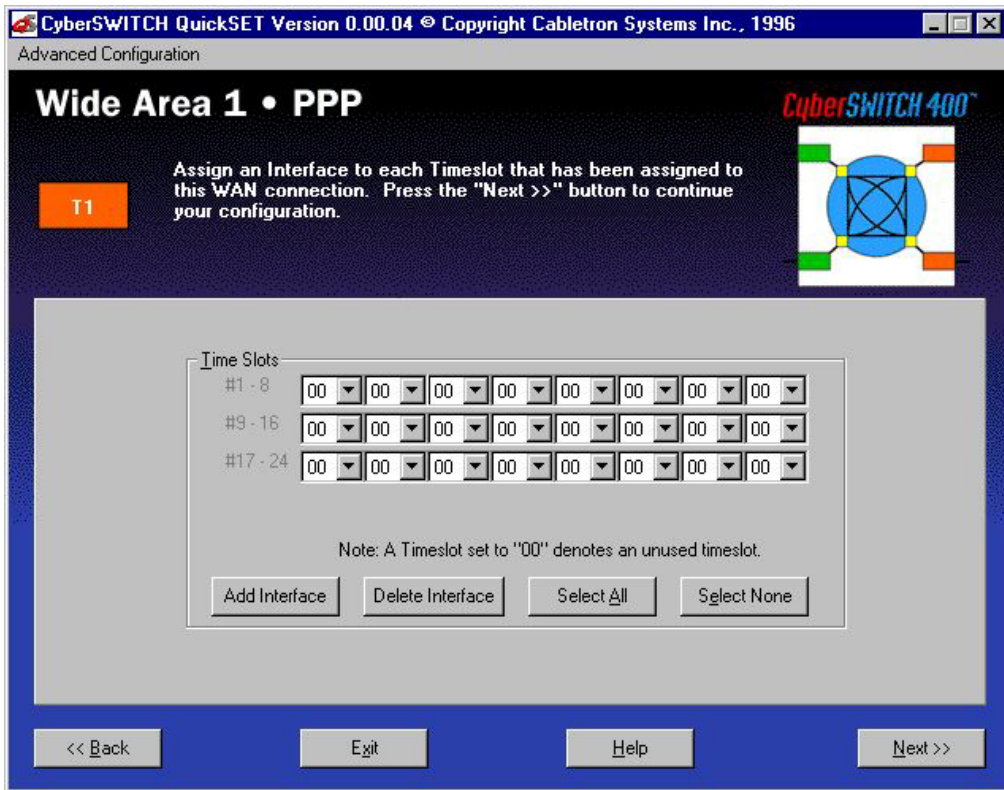
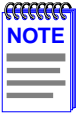


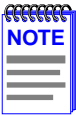
Figure 34 Wide Area PPP Time Slot Configuration Window

The following section defines the Time Slots field in the Wide Area PPP Time Slot configuration window.

Time Slots — A full line consists of 24 Time Slots (T1 and DI) or 31 Time Slots (E1) that are each capable of up to 64 Kbps throughput. Using the PPP Protocol, up to 24 interfaces (T1 and DI) or 31 interfaces (E1) can be assigned to the WAN link. Using the pull-down menu to the right of each Time Slot field, select the interface number that you wish to assign to the Time Slot.



If you are configuring a WPIM-DI Time Slot table, any available Time Slots that are set to “00” are mapped to the DI Interface. In other words, If you lease an entire T1 line, any Time Slots that are not used in the Wide Area PPP Time Slot configuration window are used by the device connected to the DI interface.



The interface numbers available in the pull-down menu are assigned in the Wide Area T1, E1, and DI configuration windows. Selecting the **Add Interface** button or the **Delete Interface** button allows available interface numbers to be added or deleted from each pull-down menu.

Once the Wide Area PPP Time Slot configuration is complete, click on the **Next>>** button, and go to the **Bridging and Routing Configuration** window.

Wide Area HDSL Time Slot Configuration Window

The Wide Area HDSL Time Slot configuration window shown in **Figure 35** displays when you click on the **Next>>** button in the Wide Area HDSL configuration window.

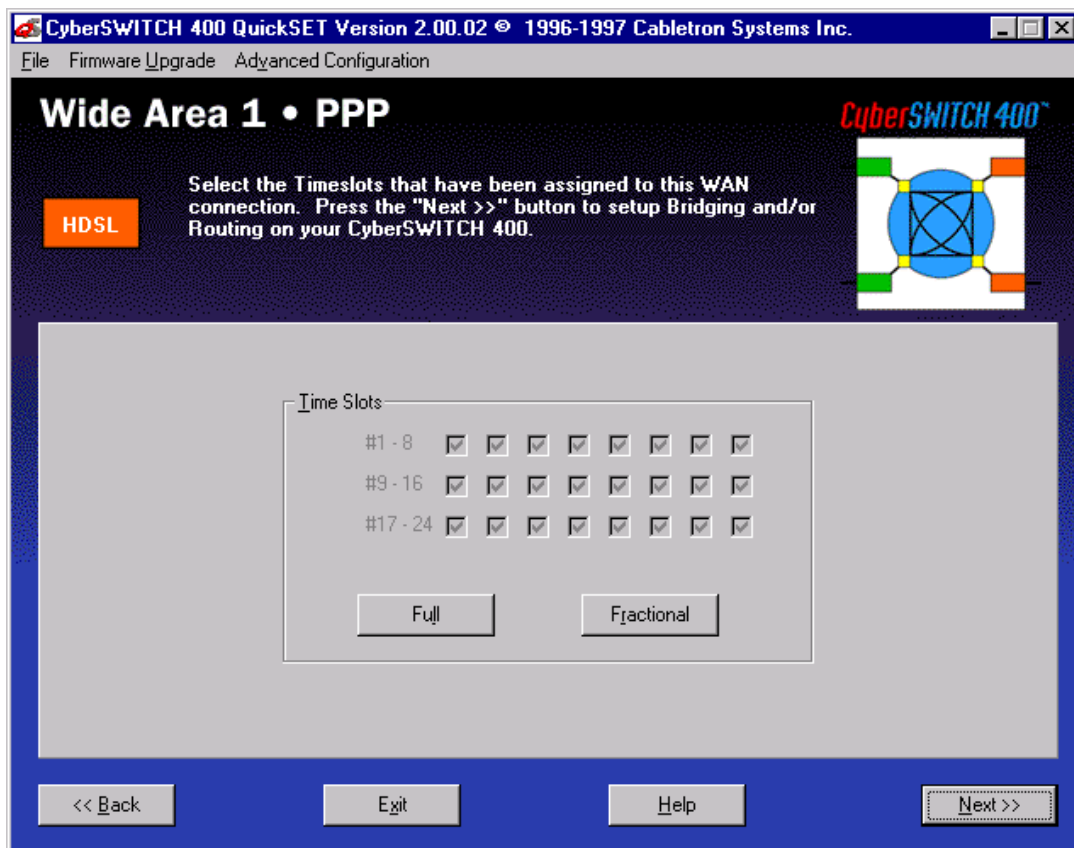


Figure 35 Wide Area HDSL Time Slot Configuration Window

The following section defines the Time Slots field in the Wide Area HDSL Time Slot configuration window.

Time Slots — A full line consists of 24 Time Slots, each capable of up to 64 Kbps throughput. If you are leasing a two pair from your service provider, you may select all the Time Slots by clicking the **Full** button. A “check mark” displays in the selected box. If you have leased one pair of a fractional line, click on the **Fractional** button to select the first 12 Time Slots.

Once the Wide Area HDSL Time Slot configuration is complete, click on the **Next>>** button, and go to the **Bridging and Routing Configuration** window.

Bridging and Routing Configuration

Once all the necessary network information is collected for the WAN, the CSX400 can be configured for inverse multiplexing **or** bridging and/or routing.

Bridging and Routing Configuration Window

The first Bridging and Routing configuration window shown in **Figure 36** displays after clicking on the **Next>>** button at the bottom of the Wide Area (Frame Relay, PPP, or HDSL) Time Slot configuration window or the Wide Area (Sync or DDS) configuration window.

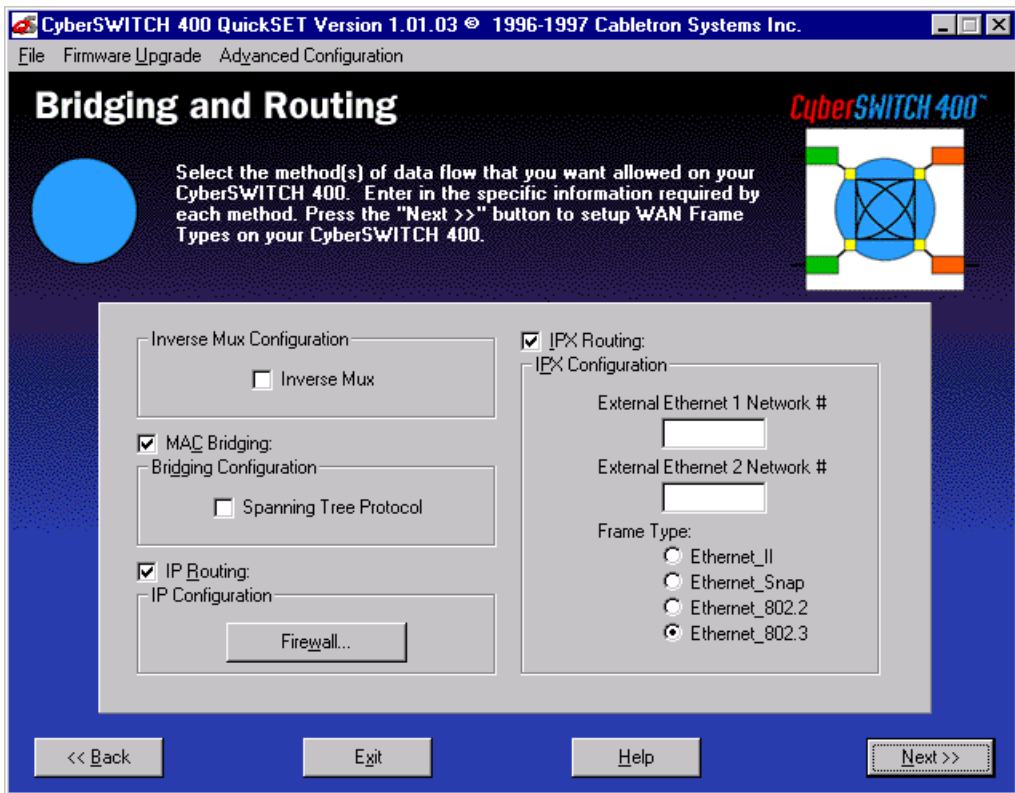
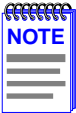


Figure 36 Bridging and Routing Configuration Window

This section describes the fields in the first Bridging and Routing configuration window.

Inverse Mux (Multiplex) Configuration — This function lets you balance your LAN traffic between two T1 WAN ports, and is used with Point to Point Protocol (PPP) or HDLC protocol. *QuickSET* automatically sets the WAN Frame Type to Encapsulated Ethernet when you use the Inverse Mux configuration. When you select the **Inverse Mux** check box, bridging, IP routing, and IPX routing functions are all disabled. The WAN device at the other end of the WAN link(s) must be a Cabletron Systems device, capable of receiving the balanced WAN traffic.



The **Inverse Mux** function is enabled or disabled through *QuickSET*, not Local Management. Statistics regarding the Inverse Mux configuration are accessed via the **imux** MIB Navigator command. See **Chapter 9, MIB Navigator**, for more information.

MAC Bridging — This field allows you to specify whether the CSX400 bridges traffic. Click on the check box to turn MAC Bridging on.

Spanning Tree Protocol — This field is grayed out until MAC Bridging is turned on. It allows you to configure the CSX400 to use the Spanning Tree Protocol, which lets the remote device check for bridging loops, and other sites that use the Spanning Tree Protocol. Click on the check box to turn on Spanning Tree Protocol.

IP Routing — The IP Routing check box allows you to turn on/off IP Routing. Click on the check box to turn on IP Routing.

IPX Routing — The IPX Routing check box allows you to turn on/off IPX Routing. Click on the check box to turn IPX Routing on.

External Ethernet 1 Network # — This field displays the IPX network number assigned to the external Ethernet network on Ethernet port 1. It is grayed out until IPX Routing is turned on.

External Ethernet 2 Network # — This field displays the IPX network number assigned to the external Ethernet network on Ethernet port 2. It is grayed out until IPX Routing is turned on.

Frame Type — This field is grayed out until IPX Routing is turned on. It allows you to select the type of IPX frame in which packets are encapsulated for transmission. Select one of the four available frame types.

Firewall Configuration Window

The Firewall configuration window shown in **Figure 37** displays after clicking on the **Firewall...** button in the first Bridging and Routing configuration window. The Firewall configuration window is used to configure an Access Control List (ACL), and to allow or deny specified IP addresses to communicate through the CSX400.

The Access Control List option allows you to create access control lists that restrict traffic to, from, or between specific IP hosts, subnets, or networks. You can configure access control restrictions based on the following:

- The source, destination, or a combination of the source and destination address of a packet.
- The upper layer protocol type of a packet such as TCP, UDP, ICMP, or all TCP/IP protocols.
- The TCP or UDP port number of a packet.

When an IP Access Control List (ACL) is enabled on a router port, each packet forwarded out this port is first checked against the ACL. If the address(es) of a packet match the address(es) in the first filter in the list, the packet is permitted or denied as specified by that filter. If there is no match, the packet is checked against the second filter, and so on, until a match is found, or until the packet has been checked against all of the filters in the list. If the packet does not match any of the filters, then the packet is permitted to pass through the port.

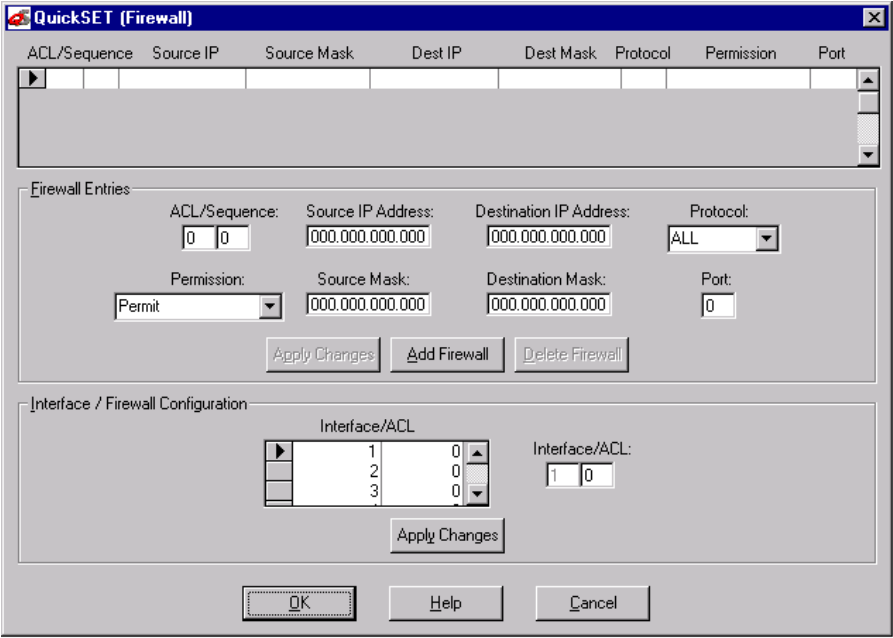


Figure 37 Firewall Configuration Window

The following definitions explain the fields in the Firewall configuration window.



The **Add Firewall** button clears the fields in the Firewall configuration window, allowing you to type in the fields as necessary. The **Apply Changes** button adds the newly entered filter to the Access Control List.

ACL (Access Control List) — The Access Control List number is a number assigned to a specific list of sequence numbers.

Sequence — A number assigned to individual access filters in an access list. As only one IP Access Control List can be applied to each port, a single list often includes several access control filters. Each filter permits or denies access to or from a certain host, subnet, or network. When an access control list contains multiple filters, the filters are referenced in order of their sequence numbers.

Source IP — The Source IP field displays the IP address of the source device accorded the permissions set in the permissions field. To set permissions for a source device, place the cursor in the Source IP field and type the IP address of the source that you wish to set permissions.

Source Mask — Displays the mask for the Source IP address specified in the Source IP field. To set the mask for the specified source IP address, place the cursor in the Source Mask field and type the mask.

The default Mask for both the source and destination addresses is 0.0.0.0, which masks the entire address, causing all addresses to match the filter. In other words, the default access control list allows all traffic to pass. Entering a mask of 255.255.255.255 causes only packets matching the exact address you have entered to match the filter.

For a Class C address, entering a mask of 255.255.255.0 causes packets with the same class C subnet as the IP address to match, thereby causing the access control filter to apply to all hosts on this particular subnet.

Dest IP — The Dest IP field displays the IP address of the destination device accorded the permissions set in the permissions field. To set permissions for a certain destination device, place the cursor in the Dest IP field and type the IP address of the destination for which you wish to set permissions.

Dest Mask — Displays the mask for the Destination IP address specified in the Dest IP field. To set the mask for the specified destination IP address, place the cursor in the Dest Mask field and type the mask.

Protocol — Use this pull-down list to select the upper layer protocol that you want to apply to the access control filter. Each access control filter can apply to traffic for all protocols included in the TCP/IP suite, or just to traffic for a single protocol.

Permission — Use this pull-down list to set the permissions for the specified control filter. Options for this field include permit, deny, permit bi-directional, or deny bi-directional. Choosing permit allows the specified packets to be forwarded, while choosing deny blocks the specified packets. Choosing permit bi-directional or deny bi-directional either permits or denies traffic to and from a specified source or destination.

Port — Enter the port number in this field to create an access control filter that applies only to traffic for a specific TCP or UDP service. **Table 19** and **Table 20** supply a list of the standardized TCP and UDP port numbers.

Table 19 TCP Services Port Numbers

TCP Services	Port #	TCP Services	Port #
FTP (File Transfer Protocol) -data	20	Host Name (NIC Host Name Server)	101
FTP	21	X.400 Mail Service	103
TELNET (Terminal Connection)	23	X.400 Mail Sending	104
SMTP (Simple Mail Transport Protocol)	25	AUTH Authentication Service	113
Time	37	UUCP-PATH Service	117
Host Name Server	42	NNTP (USENET News Transfer Protocol)	119
Domain Name Server	53	PWDGEN (Password Generator Protocol)	129
Finger	79	NETBIOS-SSN (NETBIOS Session Service)	139
HTTP	80	HTTPS (Secure)	443
DCP (Device Control Protocol)	93		

Table 20 UDP Services Port Numbers

UDP Service	Port #	UDP Service	Port #
Time	37	Bootstrap Protocol Client	68
Host Name Server	42	Trivial File Transfer	69
Domain Name Server	53	Sunrpc (NIS)	111
TACACS-Database Service	65	NETBIOS Name Server	137
Bootstrap Protocol Server	67	NETBIOS Datagram Server	138

When you have finished making changes, click on the **Apply Changes** button. Once the Firewall configuration is complete, click on the **OK** button to return to the Bridging and Routing configuration window.

Once the first part of the Bridging and Routing configuration is complete, click on the **Next>>** button, and go to the second Bridging and Routing (WAN Frame Type) configuration window.

Bridging and Routing (WAN Frame Type) Configuration Window

The second Bridging and Routing (WAN Frame Type) window shown in **Figure 38** displays after clicking on the **Next>>** button at the bottom of the first Bridging and Routing configuration window. This window is used to select a WAN Frame Type for each interface.

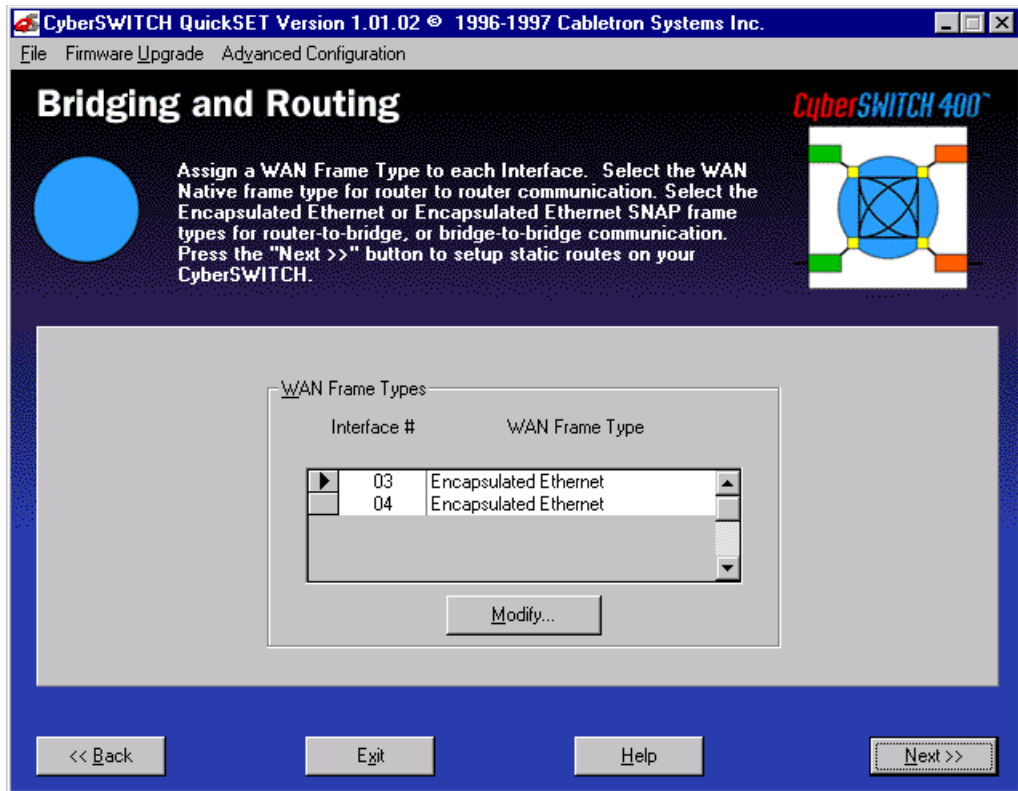


Figure 38 Bridging and Routing (WAN Frame Type) Configuration Window

The Bridging and Routing window displays fields for each interface number and its associated WAN Frame Type. Select the WAN Native frame type for router to router communication. Select the Encapsulated Ethernet or Encapsulated Ethernet SNAP frame types for router-to-bridge, or bridge-to-bridge communication.

To change the WAN Frame Type information, scroll through the list of interface entries, and select the interface number you wish to modify by pressing the arrow button on the left side of the Interface # field and press the **Modify...** button. The WAN Frame Type window displays.

The WAN Frame Type window shown in **Figure 39** allows you to select one of three frame types to be used over the WAN for each interface: Native WAN, Encapsulated Ethernet, and Encapsulated Ethernet SNAP. Select the WAN Frame Type that you wish to enable by clicking the appropriate radio button. When you are done, click the **OK** button. The OK button returns you to the Bridging and Routing (WAN Frame Type) configuration window.

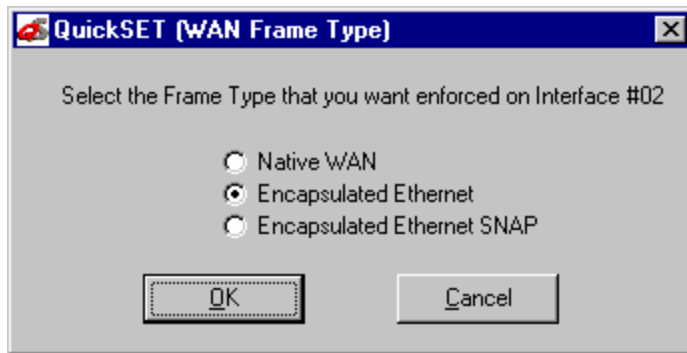


Figure 39 WAN Frame Type Configuration Window

Once the Bridging and Routing (WAN Frame Type) configuration is complete, click on the **Next>>** button, and go to the **Routing Configuration Window** section.

Routing Configuration Window

The (IP/IPX) Routing configuration window shown in **Figure 40** displays after clicking on the **Next>>** button in the second Bridging and Routing (WAN Frame Type) configuration window.

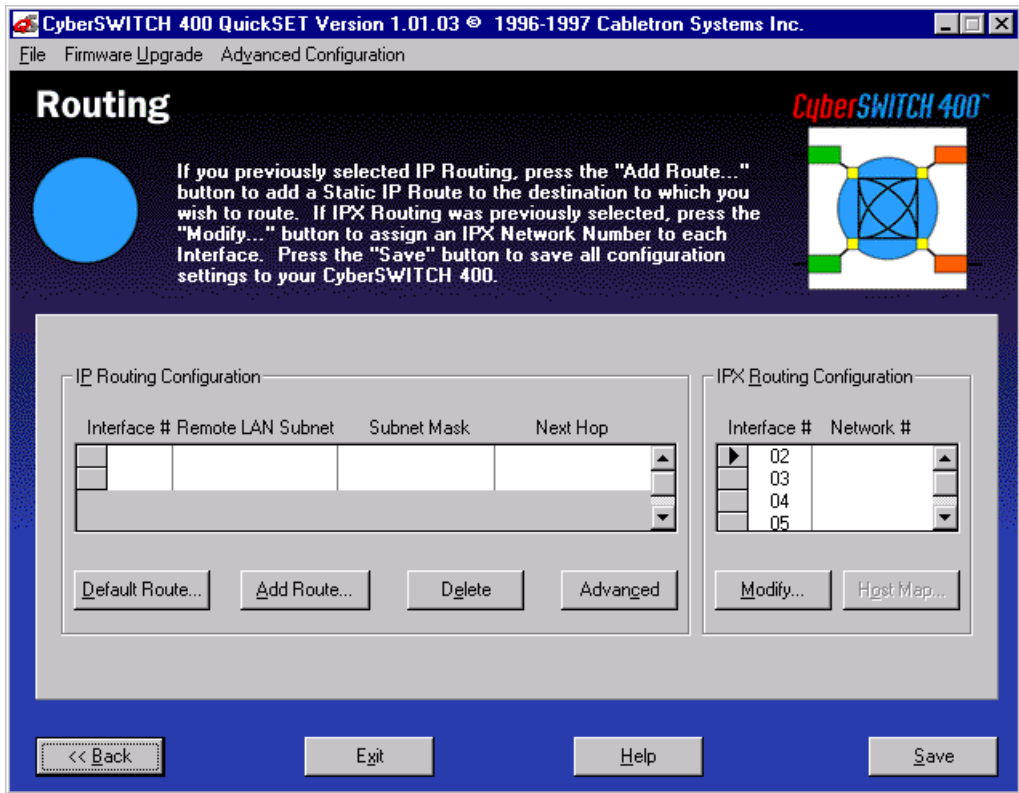


Figure 40 Routing Configuration Window

This section describes the fields in the (IP/IPX) Routing configuration window. Refer to the **IP Routing Configuration** section to configure the CSX400 for IP routing. Otherwise, refer to **IPX Routing Configuration** section to configure the CSX400 for IPX routing.

IP Routing Configuration

This section describes the fields in the IP Routing Configuration section of the Routing configuration window.

Interface # — Displays an interface number assigned an IP subnet.

Remote LAN Subnet — Displays the IP subnet assigned to the interface number.

Subnet Mask — Displays the Subnet Mask assigned to the interface number.

Next Hop — The Next Hop is the IP address of the IP port of the next router (in the direction of the subnet that you are defining).

Default Route... — Displays the Default Route window. You can select one interface to be a default route. A default route forwards all packets that are not defined in the routing table to the interface defined in the Default Route window (Unnumbered Routing Only). To set up a default route in “**Numbered Mode**” communication, click the **Add Route** button and enter IP Subnet 000.000.000.000, and Subnet Mask 255.255.255.255. Then use the **NEXT HOP** window to enter the IP Address of the router you wish to designate as the default route.

Add Route... — This button allows you to add a route and to configure the CSX400 to forward only those packets from the specified route.

Delete — This button allows you to delete a route

Advanced — This button allows you to access the Advanced Routing configuration window.

IPX Routing Configuration

This section describes the fields in the IPX Routing Configuration section of the (IP/IPX) Routing configuration window that is used to assign an IPX network number.

Interface # — Displays all interface numbers which can be assigned an IPX network number.

Network # — Displays the active IPX network number assigned to an interface.

Host Map... — The IPX Host Map button takes you to the IPX Host Map window. IPX Host Map entries are used for IPX routing in Frame Relay mode only.

Modify... — Use this button to change an entry in the IPX Routing Configuration window. Select the interface number to modify by clicking on the tab to the left of the interface number.

Host Map Window

The Host Map window shown in **Figure 41** displays after clicking on the **Host Map...** button in the (IP/IPX) Routing configuration window. Host Map entries are used for IPX routing using Frame Relay Protocol only. The IPX Host Map is a database of remote IPX hosts, defined (generally) by the WAN Network number and MAC Address, and (more specifically) by the Interface Number and Data Link Connection Identifier (DLCI). The DLCI and Interface Number define the switched connection to the Telco control office. Enter the remote WAN MAC address and the remote Router's WAN Network number.

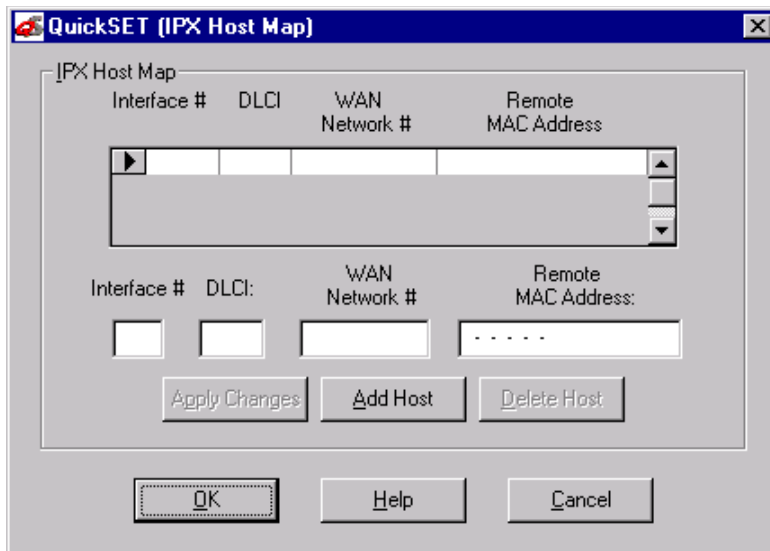


Figure 41 Host Map Window

This section describes the fields in the IP Advanced configuration window.

Interface # — Displays the active interface number. The interface number is a two-digit decimal number related to the Frame Relay Time Slot.

DLCI — Displays the Data Link Connection Identifier. Use this field to enter the DLCI, which is a four-digit decimal number corresponding to the WAN virtual circuit connection to the Telco control office.

WAN Network # — Displays the active IPX network number of the WAN connection. Use this field to enter the WAN Network number.

Remote MAC Address — Displays the remote Ethernet MAC address. Use this field to enter the remote MAC address of the device on the other end of the WAN link.

Apply Changes — Use this button to add the configured Host Map entry to the IPX Host Map list.

Add Host/Delete Host — These buttons allow you to add or delete a host and to configure the CSX400 to forward only those packets from the specified host. Use these buttons to add or delete an entry in the Host Map.

When you have finished making changes, click on the **Apply Changes** button. Click the **OK** button to exit the Host Map window and return to the (IP/IPX) Routing Configuration window.

Once your CSX400 configuration is complete, click on the **Save** button to save any configuration changes you have made. The Congratulations window displays. Click on the **OK** button to exit *QuickSET*.

Advanced Routing Configuration Window

The Advanced Routing configuration window shown in **Figure 42** displays after you click on the **Advanced** button in the (IP/IPX) Routing configuration window. Use this window to enable RIP routing, configure a Dynamic Host Configuration Protocol (DHCP) server on the CSX400, set an IP address for a remote DHCP server, or set up Network Address Translation. If you wish to run your WAN connection in Numbered Mode, enter the Local WAN IP Address Subnet Mask for Numbered Mode or leave these fields blank for Unnumbered Mode.

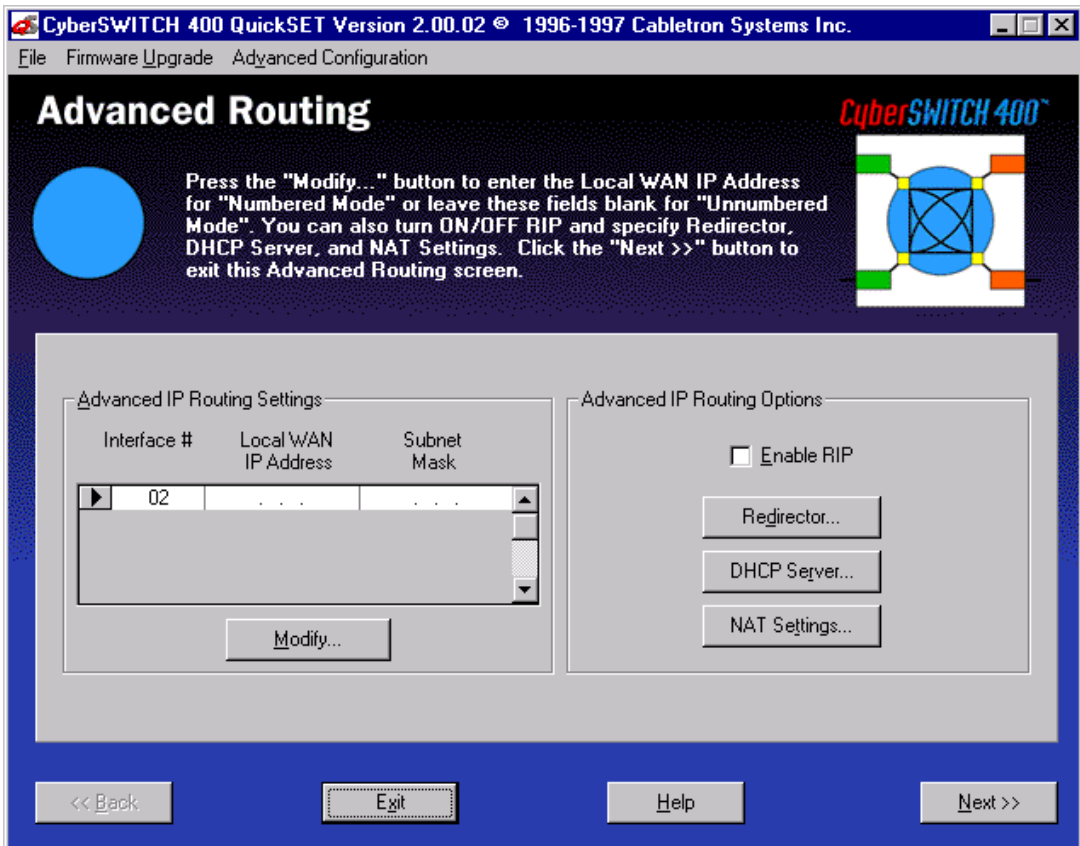


Figure 42 Advanced Routing Configuration Window

Advanced IP Routing Settings

This section describes the fields for the Advanced IP Routing Settings of the Advanced Routing configuration window.

Interface # — Displays the active interface number.

Local WAN IP Address — Set this value only if you are going to use numbered mode. In numbered mode, the Local WAN IP address is the IP address of the WAN link leading into the Telco control office. A Subnet Mask is required for this IP address before you can use this link.

Subnet Mask — Displays the subnet mask for the Local WAN IP address.

Modify — Use this button to change an entry in the Advanced IP Routing Settings box.

Advanced IP Routing Options

This section describes the fields for the Advanced IP Routing Options of the Advanced Routing configuration window.

Enable RIP — Selecting this function enables the sending and receiving of Routing Information Protocol packets. Routing Information Protocol is used in IP for broadcasting open path information between routers to keep routing tables current.

Redirector Window

The Redirector window shown in **Figure 43** displays after clicking on the **Redirector...** button in the Advanced Routing configuration window. The Redirector window is used to set up an IP address for a remote Dynamic Host Configuration Protocol (DHCP) server.

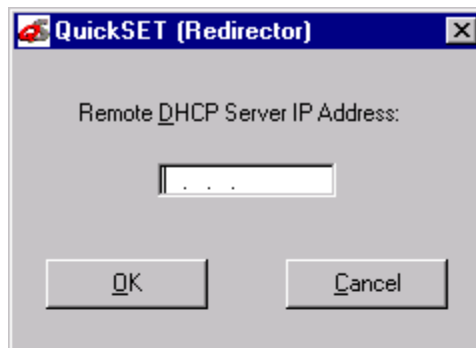


Figure 43 Redirector Window

DHCP Settings Configuration Window

The DHCP Settings configuration window shown in **Figure 44** displays after clicking on the **DHCP Server...** button in the Advanced Routing configuration window. The DHCP Settings configuration window is used to configure the DHCP settings for the CSX400.

QuickSET (DHCP Settings)

Ethernet

☐ DHCP Server is Enabled

DHCP IP Address Pool

First IP Address: . . .

Last IP Address: . . .

Default Gateway: . . .

Subnet Mask: 255.255.255.000

Lease Timeout: [dropdown]

DNS Settings

Server IP Address: . . .

Domain Name: [text box]

WINS Servers

Server IP Address: . . .

OK Cancel

Figure 44 DHCP Settings Configuration Window

The following definitions explain the fields in the DHCP Settings configuration window:

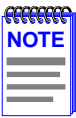
DHCP Server is Enabled — Check this box to allow the CSX400 to act as a DHCP server.

DHCP IP Address Pool — A set of contiguous IP addresses that can be assigned by the CSX400 to devices requesting an IP address.

Default Gateway — A location to send any packets that are not assigned to your subnet.

Subnet Mask — The subnet mask for the default gateway (automatically set).

Lease Timeout — Used to designate the amount of time the IP addresses in the pool can be used before they become invalid. Click on the pull-down menu to view a list of available leased timeout intervals.



Selecting **Never** allows you to keep your DHCP assigned IP address until the next time you boot up your PC.

DNS Settings — Allows you to set up an IP address and a domain name for a Domain Name server.

WINS Servers — Windows Internet Name Service (WINS) resolves NETBIOS computer names to IP addresses.

Server IP Address — Used to enter the IP address of your WINS server.

NAT Settings Configuration Window

The Network Address Translation (NAT) Settings configuration window shown in **Figure 45** displays after clicking on the **NAT Settings...** button in the Advanced Routing configuration window. The NAT Settings configuration window is used to set up Network Address Translation on Ethernet ports 1 and 2.

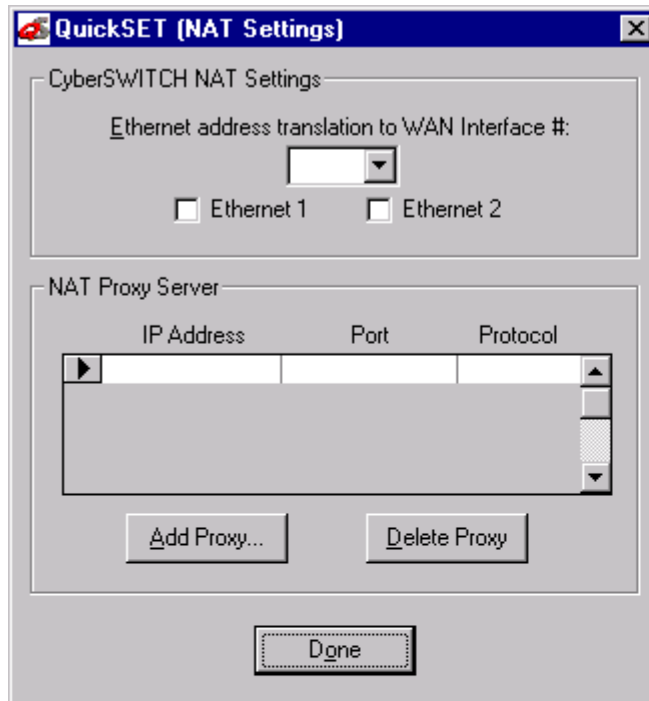


Figure 45 NAT Settings Configuration Window

The following definitions explain the fields in the NAT Settings configuration window.

Ethernet address translation to Interface # — This pull-down menu is used to disable (OFF) or enable NAT for an interface number. To enable NAT click the pull-down menu button and select an interface number to run NAT through.

Add Proxy... — Allows you to add NAT proxy servers. Click the **Add Proxy...** button and an **Add NAT Proxy Server** window (**Figure 46**) will appear. Enter an IP Address, and select a Port number/type and a Protocol for each server entry.

Delete Proxy... — Allows you to delete NAT proxy servers.

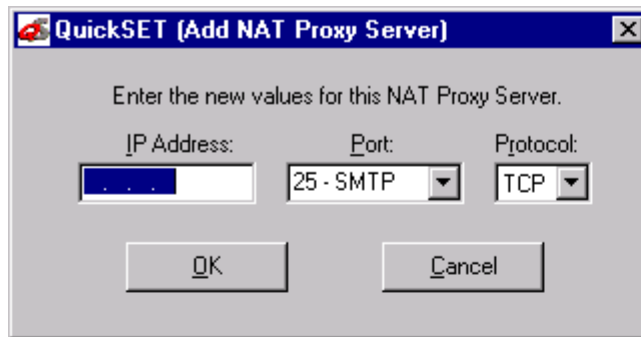


Figure 46 Add NAT Proxy Server Window

Once your CSX400 Advanced Routing configuration is complete, be sure to save any changes you make. Click on the **Next>>** button in the Advanced Routing configuration window to return to the (IP/IPX) Routing configuration window.

QuickSET Pull-Down Menus

The File, Firmware Upgrade and Advanced Configuration *QuickSET* pull-down menus allow you to store and restore configurations, initiate TFTP/BootP Services, and configure Compression and Congestion Settings for your CSX400.

File Menu

This section describes the pull-down menu options from the File menu as shown in **Figure 47**.

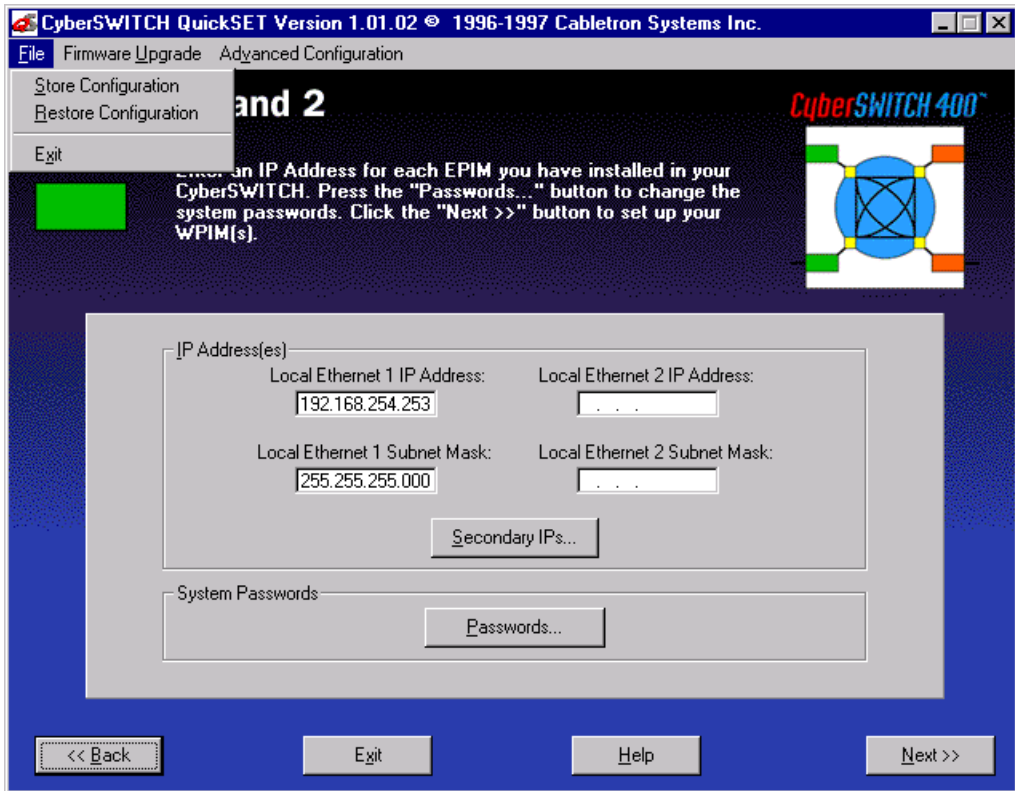


Figure 47 File Menu

Store Configuration — The Store Configuration window shown in **Figure 48** displays after clicking on the **File** pull-down menu and selecting **Store Configuration** at the top of any *QuickSET* configuration window. The Store Configuration window stores the entire CyberSWITCH configuration to a file name and drive that you specify.

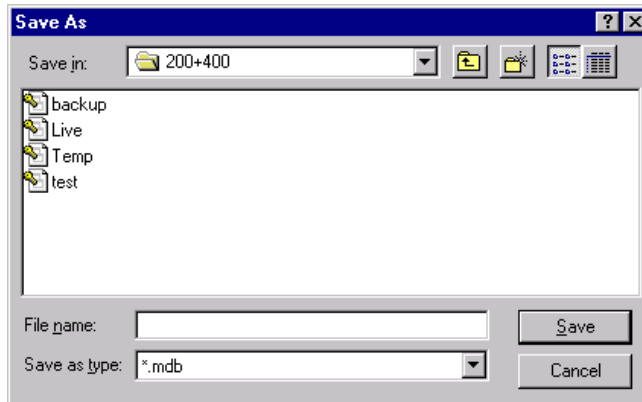


Figure 48 Store Configuration Window

Restore Configuration — The Restore Configuration window shown in **Figure 49** displays after clicking on the **File** pull-down menu and selecting **Restore Configuration** at the top of any *QuickSET* configuration window. The Restore Configuration window allows you to load your stored configuration from a drive into *QuickSET* where it can be loaded into your CyberSWITCH and saved.

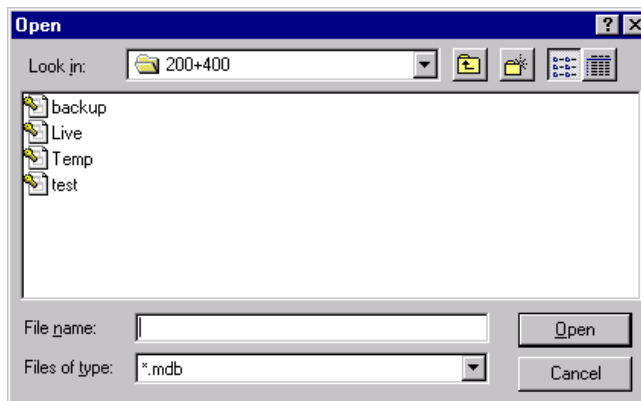


Figure 49 Restore Configuration Window

Firmware Upgrade Menu

This section describes the pull-down menu option available from the Firmware Upgrade menu as shown in **Figure 50**.

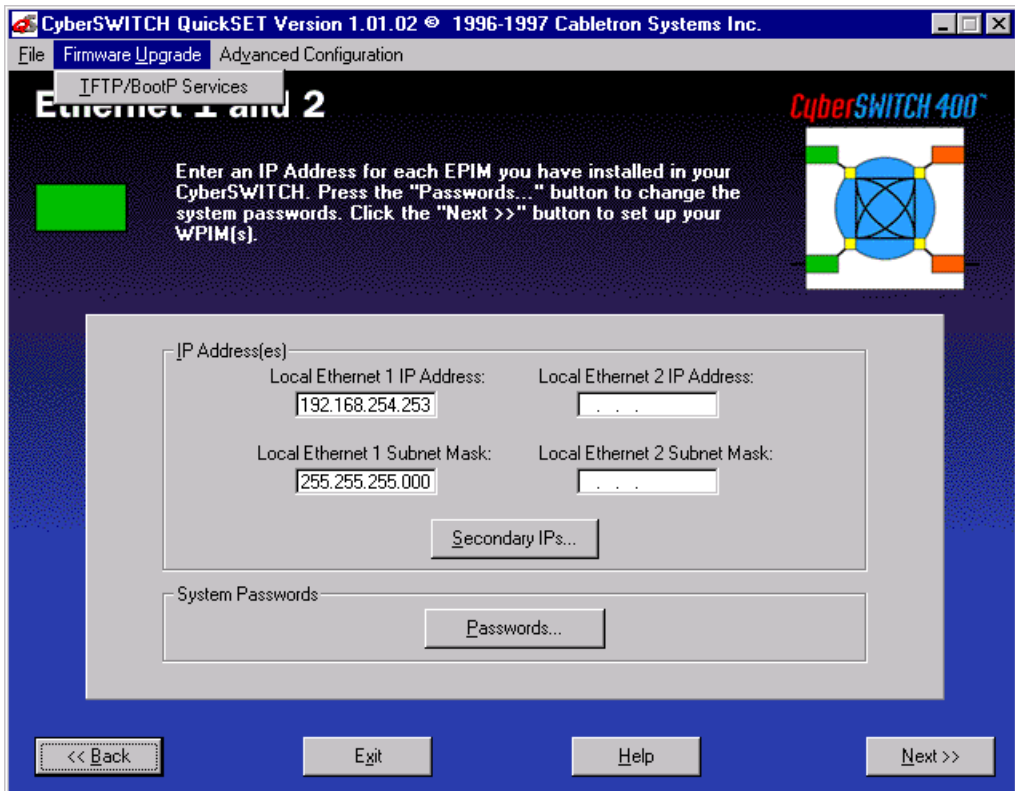


Figure 50 Firmware Upgrade Menu

TFTP/BootP Services — The TFTP/BootP Services window shown in **Figure 51** displays after clicking on the **Firmware Upgrade** pull-down menu and selecting **TFTP/BootP Services** at the top of any *QuickSET* configuration window. The TFTP/BootP Services window allows you to access a TFTP (Trivial File Transfer Protocol) server or BootP server to download the latest version of CSX400 firmware.

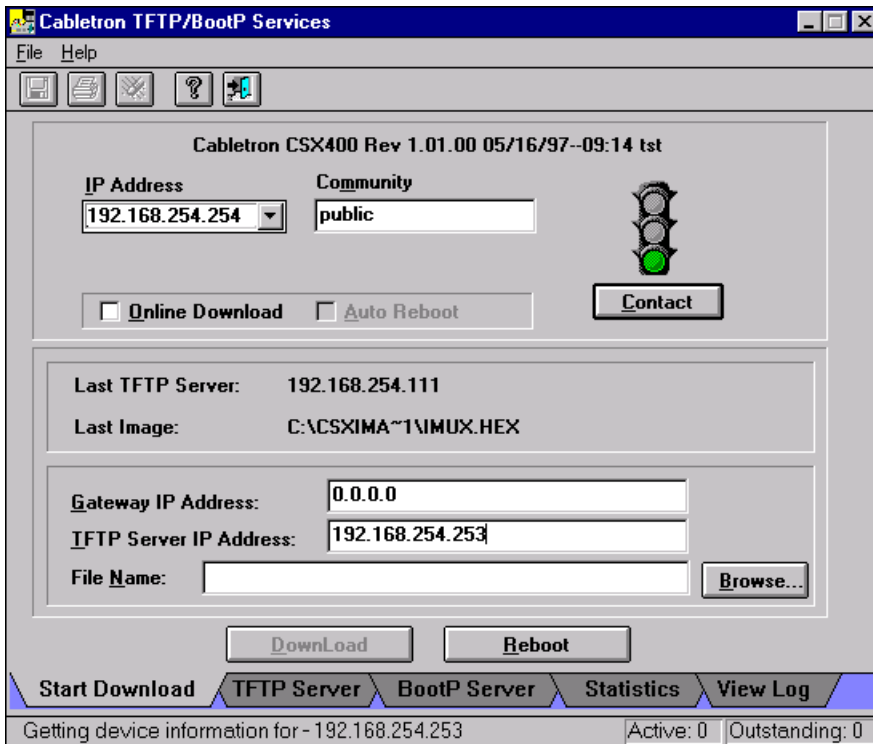


Figure 51 TFTP/BootP Services Window

This section describes the modifiable fields of the TFTP /BootP Services window:

IP Address — The IP Address field shows the IP Address of the CSX400 to which you are upgrading the firmware.

Community — The Community field allows you to enter the password of your CSX400.

Gateway IP Address — Use the Gateway IP Address field to enter the IP Address of the server acting as a gateway between the CSX400 and the TFTP server.

TFTP Server IP Address — The TFTP Server Address indicates the IP address of the PC running this utility.

File Name — The File Name field indicates the location and name of the firmware image you are putting on your CSX400.

Download — The DownLoad button starts the firmware download to your CSX400.

Advanced Configuration Menu

This section describes the pull-down menu options available from the Advanced Configuration menu as shown in [Figure 52](#).

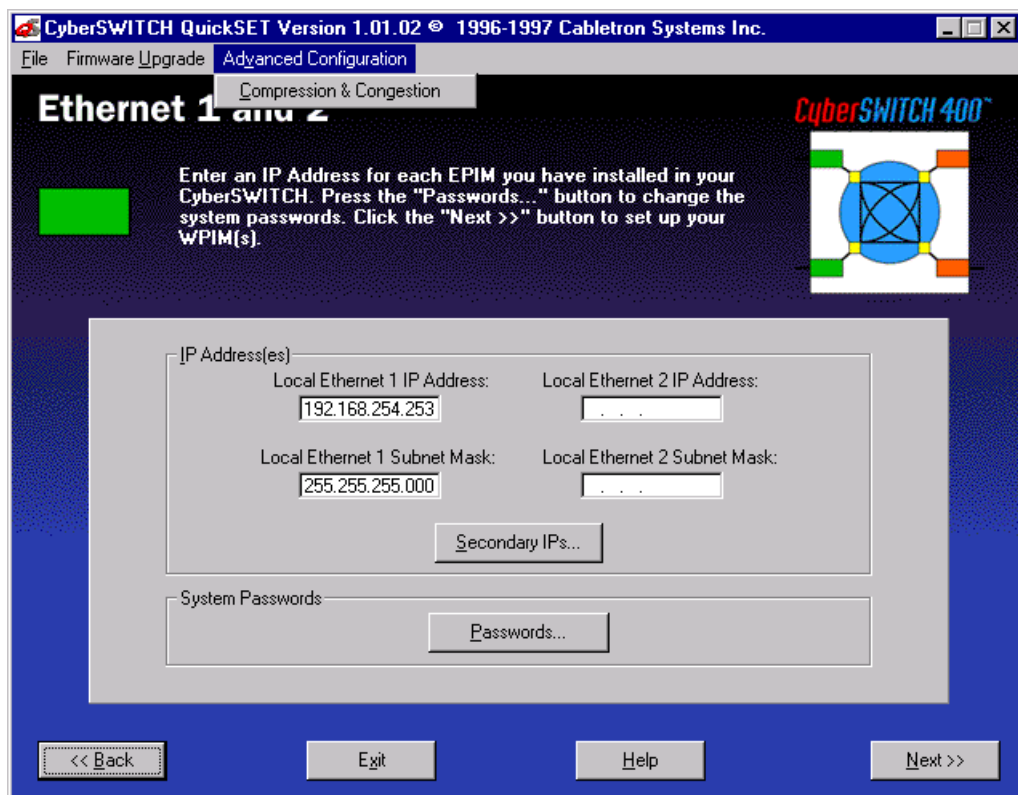


Figure 52 Advanced Configuration Menu

Compression and Congestion Window

The Compression and Congestion window shown in **Figure 53** displays after you click on the **Advanced Configuration** pull-down menu and select **Compression & Congestion** at the top of any *QuickSET* configuration window.

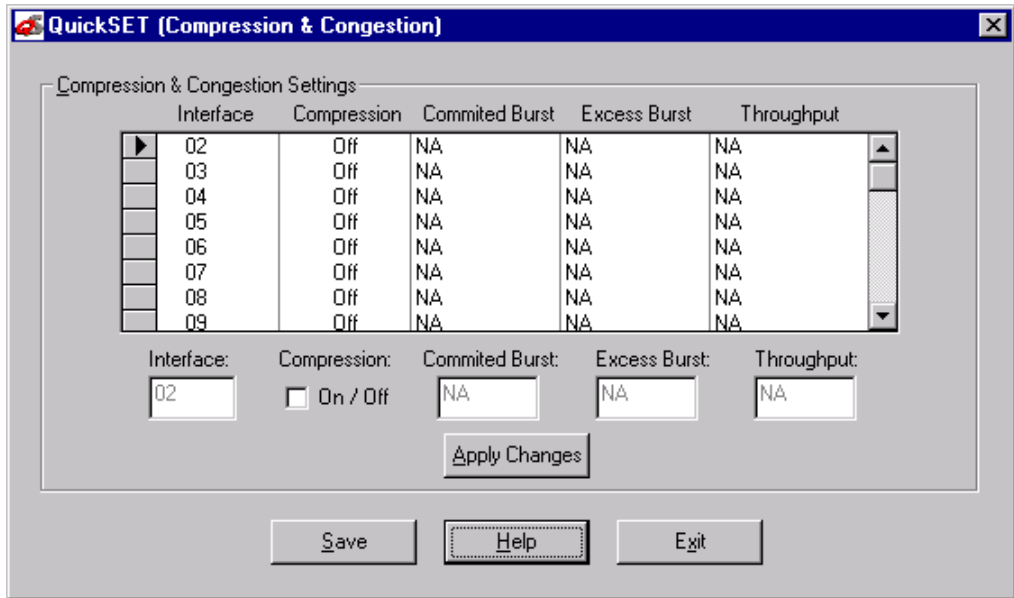


Figure 53 Compression and Congestion Window

The Compression and Congestion window allows you to enable data compression on each interface. Data compression allows the size of the data being sent on a WAN link to be minimized, making the WAN link more efficient. To use data compression, the CSX400 must first be fully configured and connected to a live WAN link, and compression must be configured on any remote WAN device(s). Using software compression, the CSX400 supports up to four DS0s (256 Kbps) per WPIM. With the optional hardware compression module installed, the CSX400 supports data compression on all DS0s, which is equivalent to two full T1 lines. For more information on the hardware data compression module (CSX-COMP/ENCR) refer to **Chapter 2**,

The following defines the fields in the Compression and Congestion window.

Interface — Displays the available, pre-configured interface numbers.

Compression — Displays the status of data compression for a specific interface. Options for this field are either on (box shows a check mark) or off.

The following defines the fields for Frame Relay only:

Committed # Burst — Displays the Committed Burst size, which is the maximum amount of data a user may offer to the network during a calculated time interval. Data is guaranteed not to be discarded by the network.

Excess # Burst — Displays the Excess Burst size, which is the maximum amount of data by which a user can exceed the Committed Burst size. This data is not guaranteed to be passed by the network.

Throughput — Displays the maximum bandwidth of your WAN connection.

To turn data compression on or off for a specific interface, click on the interface number that you wish to configure in the compression scroll list, then click the compression check box. Clicking the **Apply Changes** button applies the changes to the interface.

Once compression configuration is complete, click on the **S**ave button to save any changes you make, then click on the **E**xit button to exit the Compression and Congestion window.

8

General Configuration Using Local Management

This chapter explains how to access and manage the CSX400 and its attached segments through a TELNET connection. A general working knowledge of basic network operations and an understanding of management applications is helpful prior to using Cabletron Systems Local Management.

This chapter describes how to perform the following:

- Access the CSX400 through a TELNET application
- Identify and operate the types of fields used by Management
- Navigate through Management fields and menus
- Use Management screens to perform management operations

Chapter Organization

The following list summarizes the organization of this chapter:

Local Management Overview outlines the contents of this chapter, provides an overview of Local Management, and explains how to use the management screens.

Accessing Local Management describes how to access the Main Menu screen and navigate through the Local Management screens.

System Level Screen describes how to use the System Level screen, its functions, and operations.

SNMP Community Names Screen explains how to control access to the CSX400 by assigning community names.

SNMP Traps Screen explains how to configure the CSX400 to send SNMP traps to multiple network management stations.

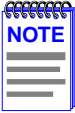
Flash Download Screen describes how to download new firmware to the CSX400.

Bridge Setup Screen describes how to configure the CSX400 for bridge functions.

IP Configuration Screen describes how to configure the CSX400 for IP routing functions.

IPX Configuration Screen describes how to configure the CSX400 for IPX routing functions.

WAN Setup describes how to configure the CSX400 for a Wide Area Network (WAN) interface.



If you have a WPIM-HDSL installed in your CSX400, refer to the WAN Setup section of this chapter for configuration information. For all other WPIMs, refer to your specific WPIM(s) Local Management Guide for information on this screen.

Local Management Overview

Cabletron Systems Local Management is a management tool that allows a network manager to perform the following tasks:

- Configure interconnected devices to form a network.
- Monitor the performance of the network.
- Control user access to the network and its components for the purpose of security.

Management Agent

The management agent is a process within the CSX400 that collects information about the operational performance of the managed network. Local Management communicates with the management agent for the purpose of issuing management commands to network devices.

Local vs. Remote Management

Network management applications are usually described as either local or remote management applications. A Local Management application resides within the circuits of the CSX400 management agent and is accessible by making a TELNET connection through one of the two EPIM ports located on the front panel of the device. Remote management applications such as Cabletron Systems **SPECTRUM**, **SPECTRUM Element Manager**, or **QuickSET** run in another device that provides management services. This allows you to perform network management from a remote location.

Local Management Screen Elements

There are five basic field elements shown in the Local Management screen in **Figure 54**.

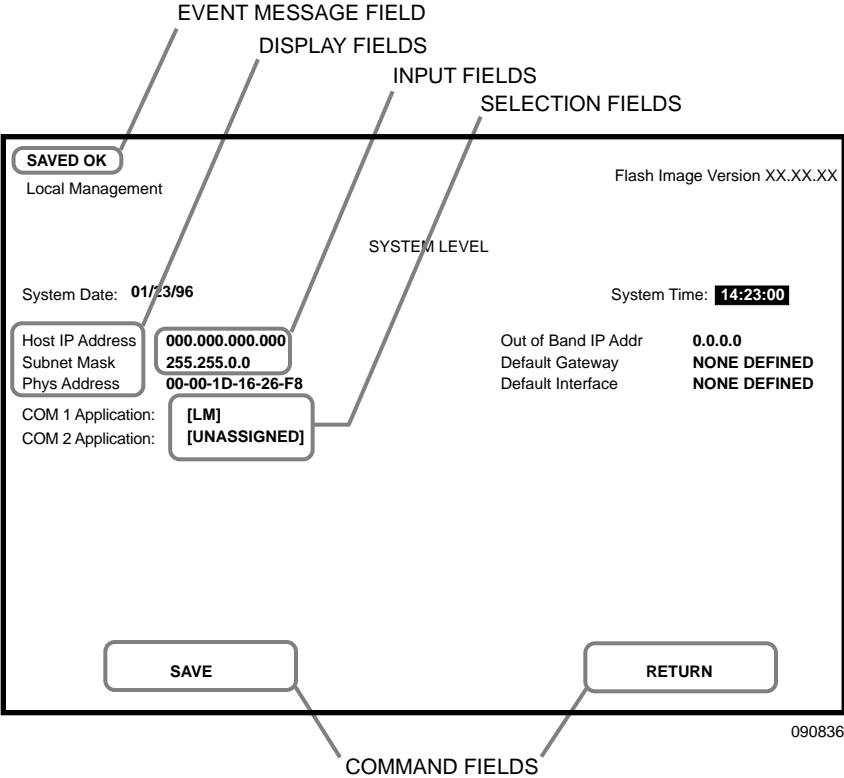


Figure 54 Sample Local Management Screen

The following list explains each of the basic Local Management screen fields:

Event Message Field — This field briefly displays messages that indicate if a Local Management procedure was executed correctly or incorrectly, that changes were saved or not saved to Non-Volatile Random Access Memory (NVRAM), or that a user did not have access privileges to an application.

Table 21 describes the most common event messages. Event messages related to specific Local Management applications are described with those applications throughout this manual.

Table 21 Event Messages

Message	Meaning
SAVED OK	One or more fields were modified, and saved to NVRAM.
NOT SAVED?--PRESS SAVE TO KEEP CHANGES	One or more fields were modified, but not yet saved to NVRAM.
NOTHING TO SAVE	The SAVE command was executed, but nothing was saved to NVRAM.

Display Fields — Display fields cannot be edited. These fields may display information which never changes, or changes as the result of Local Management operations, user selections, or network monitoring information.

Input Fields — Input fields require keyboard characters to be entered. IP addresses, System Date, and System Time are examples of Input fields.

Selection Fields — Selection fields provide a series of possible values. Only applicable values appear in Selection fields.

Command Fields — Command fields are located at the bottom of Local Management screens. Command fields are used to exit Local Management screens and to save Local Management entries. Command fields perform a management action simply by being selected and activated. Only command fields can make a change to a device’s configuration.

Local Management Keyboard Conventions

All key names in this manual display as capital letters. For example, the ENTER key displays as ENTER, the Escape key displays as ESC, and the Backspace key displays as BACKSPACE.

Table 22 explains the keyboard conventions used in this manual as well as the key functions.

Table 22 Keyboard Conventions

Key	Function
ENTER and RETURN	These selection keys perform the same Local Management function. For example, “Press ENTER” means that you can press either ENTER or RETURN, unless this manual specifically instructs you otherwise.
ESC	This key lets you escape from a Local Management screen without saving your changes. For example, “Press ESC twice” means that you must quickly press the ESCAPE key two times to exit the Local Management screen.
SPACE bar and BACKSPACE	These keys cycle through selections in some Local Management fields. Press the SPACE bar to cycle forward through selections and press BACKSPACE to cycle backward through selections.
Arrows	These are navigation keys. Use the UP-ARROW, DOWN-ARROW, LEFT-ARROW, and RIGHT-ARROW keys to move the screen cursor. For example, “Use the arrow keys” means to press whichever arrow key moves the cursor to the desired field on the Local Management screen.
SHIFT-[+/=]	This key combination increments values in some Local Management selection fields. For example, “Press SHIFT-[+/=]” means to hold down the SHIFT key while pressing the PLUS/EQUAL key.
[-]	This key decreases values from some Local Management selection fields. For example, “Press [-]” means to press the MINUS key.
DEL	The DEL (Delete) key removes characters from a Local Management Selection field. For example, “Press DEL” means to press the DELETE key.

Navigating Within Local Management Screens

To navigate within a Local Management screen, use the arrow keys of the terminal or the workstation providing terminal emulation services. The Local Management screen cursor responds to the LEFT-ARROW, RIGHT-ARROW, UP-ARROW, and DOWN-ARROW keys. Each time you press an arrow key, the Local Management screen cursor moves to the next available field in the direction of the arrow key.

The Local Management screen cursor only moves to fields which can be selected or used for input. This means that the cursor jumps over display fields and empty lines on the Local Management screen.

The Local Management screen cursor provides wrap-around operation. This means that a cursor located at the edge of a screen, when moved in the direction of that edge, “wraps around” to the outermost selectable item on the opposite side of the screen which is on the same line or column.

Selecting Local Management Menu Screen Items

To select items in a Local Management menu screen, perform the following steps:

1. Use the arrow keys to highlight a menu item.
2. Press ENTER. The selected Local Management menu screen displays.

Exiting Local Management Screens

To exit any of the Local Management screens, perform the following steps:

1. Use the arrow keys to highlight the **RETURN** command at the bottom of the Local Management screen.
2. Press ENTER. The previous screen in the Local Management hierarchy displays.



You can also exit Local Management screens by pressing ESC twice. This exit method does not warn you about unsaved changes and all unsaved changes are lost.

Exiting the Local Management Session

To exit from CSX400 Local Management, perform the following steps:

1. Use the arrow keys to highlight the **RETURN** command at the bottom of the Local Management screen.
2. Press ENTER. The previous screen in the Local Management hierarchy displays.

3. Repeat steps 1 and 2 until the Main Menu screen displays.
4. Use the arrow keys to highlight the **EXIT** command at the bottom of the Main Menu screen.
5. Press ENTER. The CSX400 Local Management Password screen displays and the Local Management session ends.

Establishing a TELNET Connection

The CSX400 is shipped with a temporary IP Address of **192.168.254.254** so that your computer can communicate with it over your Local Area Network (LAN) through a TELNET connection. However, to establish a TELNET connection, your computer must be on the same subnet as the CSX400. Cabletron Systems recommends that you assign a temporary IP Address of **192.168.254.253** to your computer to ensure that both devices are on the same subnet. TELNET connections to the host device require the community name passwords assigned at the SNMP Community Names screen or if you are doing an initial configuration, use the default password *public*. Refer to the SNMP Community Names section of this manual for additional information about community names.



See the instructions included with the TELNET application for information about establishing a TELNET session.

Local Management Screen Hierarchy

Local Management consists of a series of menu screens that provide a path to each of the Local Management function screens. Navigate through Local Management by selecting items from the menu screen. **Figure 55** shows the hierarchy of the Local Management screens.

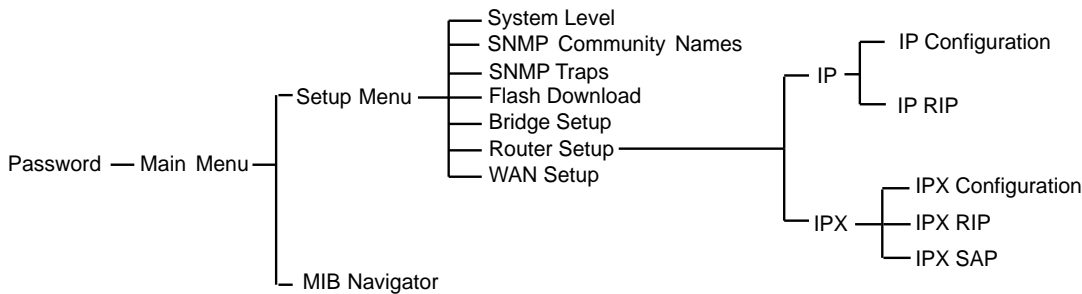


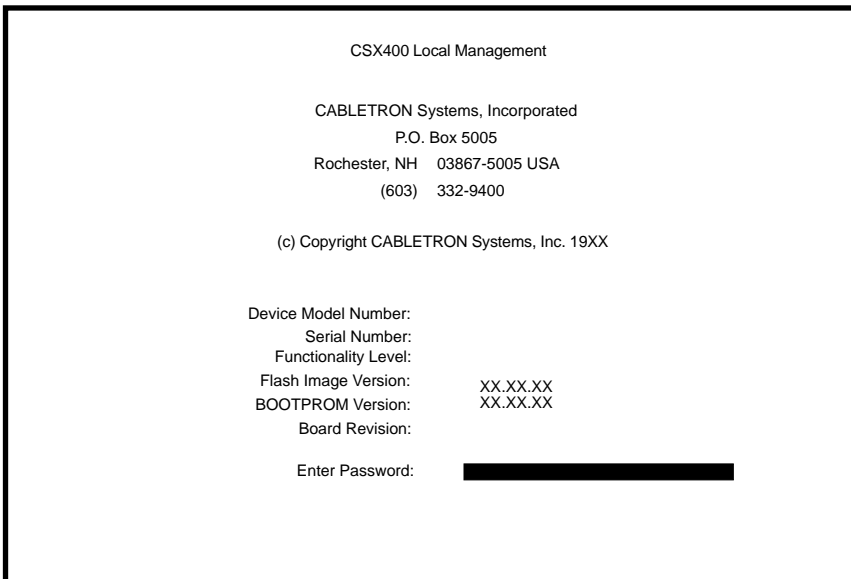
Figure 55 Hierarchy of Local Management Screens

Accessing Local Management

This section explains how to access and use the Local Management menu screens. Menu screens provide a path to the setup screens and status screens.

Using the Menu Screens

Once you have accessed the CSX400 through a TELNET connection, the CSX400 Password screen, shown in **Figure 56**, displays.

The image shows a terminal window titled "CSX400 Local Management". It contains the following text: "CABLETRON Systems, Incorporated", "P.O. Box 5005", "Rochester, NH 03867-5005 USA", "(603) 332-9400", and "(c) Copyright CABLETRON Systems, Inc. 19XX". Below this, it lists device information: "Device Model Number:", "Serial Number:", "Functionality Level:", "Flash Image Version: XX.XX.XX", "BOOTPROM Version: XX.XX.XX", and "Board Revision:". At the bottom, it says "Enter Password:" followed by a black rectangular input field.

```
CSX400 Local Management

CABLETRON Systems, Incorporated
P.O. Box 5005
Rochester, NH 03867-5005 USA
(603) 332-9400

(c) Copyright CABLETRON Systems, Inc. 19XX

Device Model Number:
Serial Number:
Functionality Level:
Flash Image Version:    XX.XX.XX
BOOTPROM Version:      XX.XX.XX
Board Revision:

Enter Password: [REDACTED]
```

Figure 56 CSX400 Password Screen

Type in your password and press ENTER. If you are doing an initial configuration, the default super-user access password is “*public*” or press ENTER.



Your password is one of the community names specified in the SNMP Community Names screen. Access to certain Local Management capabilities depends on the degree of access accorded that community name. See the SNMP Community Names section.

- If you enter a valid password, the associated access level displays at the bottom of the screen and the Main Menu screen, shown in **Figure 57**, displays.

- If you enter an invalid password, the cursor returns to the beginning of the password entry field.
- If no activity occurs for several minutes, the Password screen displays again, ending your current session. You must reenter the password to perform Local Management tasks.

Main Menu Screen

The Main Menu screen is the starting point from which all the Local Management screens are accessed. **Figure 57** shows the Main Menu screen.

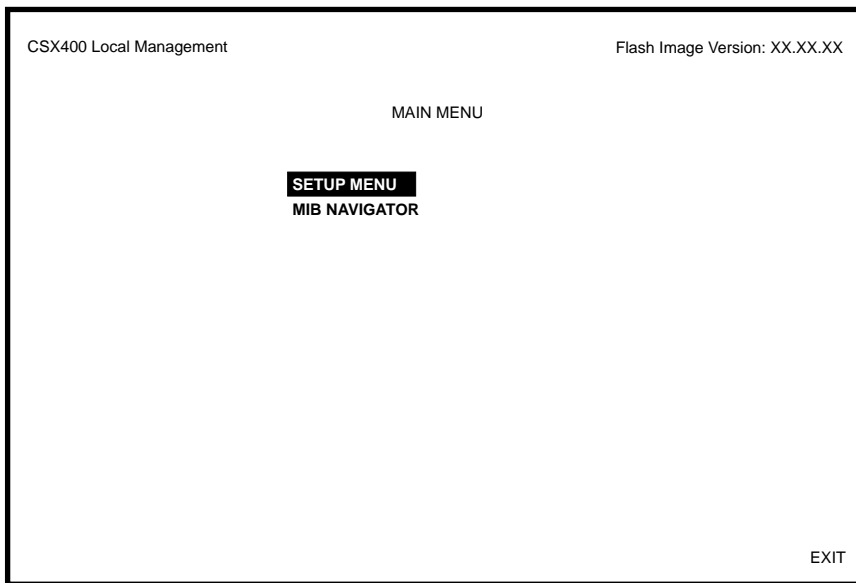


Figure 57 Main Menu Screen

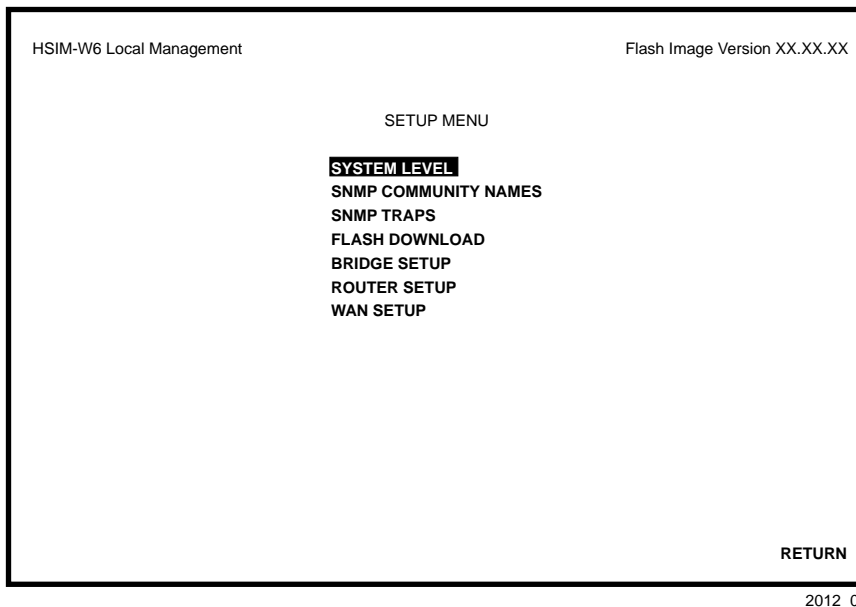
The Main Menu screen displays the following menu items:

Setup Menu — The Setup Menu provides access to Local Management screens that are used to configure the CSX400.

MIB Navigator — The MIB Navigator is a Local Management utility that allows the user to access, monitor, and set specific Management Information Base (MIB) items within the CSX400. Refer to **Chapter 9, MIB Navigator**, for information on the MIB Navigator.

Setup Menu Screen

The Setup Menu screen provides access to the Local Management screens that are used to configure the CSX400. Examples of functions accessible through the Setup Menu include configuring the host IP address and Subnet Mask, assigning the SNMP community names, and configuring the SNMP trap notification. **Figure 58** shows the Setup Menu.



2012_03

Figure 58 Setup Menu Screen

The Setup Menu screen displays the following menu items:

System Level — The System Level screen allows you to configure basic operating parameters for the CSX400.

SNMP Community Names — The SNMP Community Names screen allows you to change or review the community names used as access passwords for local management operation.

SNMP Traps — The SNMP Traps screen provides display and configuration access to the table of IP addresses used for trap destinations and associated community names.

Flash Download — The Flash Download screen allows you to download a firmware image from a TFTP server to the CSX400.

Bridge Setup — The Bridge Setup screen allows you to select a Spanning Tree protocol and enable/disable switch ports.

Router Setup — The Router Setup screen accesses two other screens that provide general IP or IPX routing configuration and allow you to enable or disable the Routing Information Protocol (RIP) and the Service Advertisement Protocol (SAP) features.

WAN Setup — The WAN Setup menu item accesses two other screens that provide WAN physical configuration and WAN Interface configuration access to enable a WAN link to be set up.



If you have a WPIM-HDSL installed in your CSX400, refer to the WAN Setup section of this chapter for configuration information. For all other WPIMs, refer to your specific WPIM(s) Local Management Guide for information on configuring the CSX400 for a Wide Area Network Interface.

System Level Screen

The System Level screen displays the physical address (MAC address) of the CSX400 and allows you to set the following parameters:

- System Date
- System Time
- Host IP Address
- Subnet Mask
- Default Gateway
- Default Interface

General Configuration Using Local Management

Access the System Level screen (**Figure 59**) from the Setup Menu screen by using the arrow keys to highlight the **System Level** option and pressing ENTER. The System Level screen displays.

CSX400 Local Management

Flash Image Version XX.XX.XX

SYSTEM LEVEL

System Date: 12/30/97

System Time: 14:23:00

Host IP Address0.0.0.0

Subnet Mask255.255.0.0

Phys Address00-00-1D-16-26-F8

Default Gateway

Default Interface

NONE DEFINED

NONE DEFINED

COM 1 Application: [LM]

SAVE

RETURN

2012_04

Figure 59 System Level Screen

The following definitions explain each System Level screen field. The sections which follow these definitions explain the use of these fields.

System Date — Use this field to enter the system date, as described in **Setting the System Date**.

System Time — Use this field to enter the system time, as described in **Setting the System Time**.

Host IP Address — Use this field to enter the IP address of the CSX400, as described in **Setting the Host IP Address**.

Subnet Mask — This field displays the default Subnet Mask, and allows you to enter a new value for the Subnet Mask if necessary. Subnets are logical divisions of the network that isolate groups of devices. The Subnet Mask determines how the CSX400 directs SNMP traps to a management workstation. If the CSX400 resides on the same network as the management workstation, then the CSX400 sends SNMP traps directly to the management workstation. If the CSX400 resides on a different subnet as the management workstation, then the CSX400 sends SNMP traps to a gateway or router.

- When the management workstations designated to receive SNMP traps reside on the same network as the CSX400, use the Subnet Mask default setting for the IP address entered on the System Level screen.
- Set a new value for the Subnet Mask when the management workstations designated to receive SNMP traps reside on a different subnet (for example, across a gateway or router)

To set a Subnet Mask, refer to the **Setting the Subnet Mask** section.

Phys Address — This field displays the physical address of the CSX400. You cannot modify the physical address.

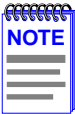
Default Gateway — Use this field to enter the Default Gateway for the CSX400. When routing packets, the CSX400 uses the IP Forwarding Table to find the route to each destination address. The IP Forwarding Table contains the routes to all networks and hosts within a certain area. However, the IP Forwarding Table on its own cannot provide all of the routes that may be needed. The CSX400 relies on a Default Gateway to provide the routes to destinations that are not listed in its own IP Forwarding Table. The Default Gateway is the IP address of the network device (gateway or router) used to forward SNMP traps to a management station. The default setting for this field is NONE DEFINED. To set the Default Gateway, refer to **Setting the Default Gateway**.

Default Interface — Use this field to select the default interface for the CSX400 Default Gateway. The default interface is the channel which is set up to handle SNMP traps sent to an IP station that is not on the same subnet as the CSX400 in an IP routed environment. The default setting for this field is NONE DEFINED. To set the default interface for the Default Gateway of the CSX400, refer to **Setting the Default Interface**.

Setting the System Date

The CSX400 is year 2000 compliant so that the System Date field can be set beyond the year 1999. To set the system date, perform the following steps:

1. Use the arrow keys to highlight the **System Date** field.
2. ENTER the date in an MM/DD/YY YY format.



When entering the date in the system date field, you do not need to add separators between month, day, and year numbers, as long as each entry uses two decimal numbers. For example, to set the date to 03/17/1997, type “03171997” in the System Date field.

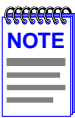
3. Press ENTER to set the system date.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER.

If the date entered was a valid format, the Event Message field at the top of the screen displays “SAVED OK”. If the entry was not valid, Local Management does not alter the current value and refreshes the System Date field with the previous value.

Setting the System Time

To set the system time, perform the following steps:

1. Use the arrow keys to highlight the **System Time** field.
2. ENTER the time in a 24-hour format, HH:MM:SS.



When entering the time in the system time field, you do not need to add separators between hours, minutes, and seconds, as long as each entry uses two decimal numbers. For example, to set the time to 6:45 a.m., type “064500” in the System Time field.

3. Press ENTER to set the system time.
4. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen and press ENTER. If the time entered was a valid format, the Event Message field at the top of the screen displays “SAVED OK”. If the entry was not valid, Local Management does not alter the current value and refreshes the System Time field with the previous value.

Setting the Host IP Address

To set the host IP address, perform the following steps:

1. Use the arrow keys to highlight the **Host IP Address** field.
2. Enter the IP address using Decimal Dotted Notation (DDN) format.
For example: 134.141.25.17
3. Press ENTER. If the IP address entered was a valid format, the cursor returns to the beginning of the Host IP Address field. If the entry was not valid, the Event Message field displays “INVALID IP ADDRESS OR FORMAT ENTERED”. Local Management does not alter the current value and refreshes the Host IP Address field with the previous value.
4. Use the arrow keys to highlight the **SAVE** command field.
5. Press ENTER. The Event Message field at the top of the screen displays “SAVED OK”.

Setting the Subnet Mask

Subnets are logical divisions of the network. To change the Subnet Mask from its default value, perform the following steps:

1. Use the arrow keys to highlight the **Subnet Mask** field.
2. Enter the Subnet Mask using Dotted Decimal Notation (DDN) format. Values for each decimal can be from 0 to 255.
For example: 255.255.0.0
3. Press ENTER. If the Subnet Mask entered was a valid format, the cursor returns to the beginning of the Subnet Mask field. If the entry was not valid, the Event Message field displays “INVALID SUBNET MASK OR FORMAT ENTERED”. Local Management does not alter the current value and refreshes the Subnet Mask field with the previous value.
4. Use the arrow keys to highlight the **SAVE** command field.
5. Press ENTER. The Event Message field at the top of the screen displays “SAVED OK”.

Setting the Default Gateway

To set the Default Gateway, perform the following steps:

1. Use the arrow keys to highlight the **Default Gateway** field.

General Configuration Using Local Management

2. ENTER the IP address of the Default Gateway using DDN format.

For example: 134.141.79.121

3. Press ENTER. If the Default Gateway address entered was a valid format, the cursor returns to the beginning of the Default Gateway field. If the entry was not valid, the Event Message field displays “INVALID DEFAULT GATEWAY OR FORMAT ENTERED”. Local Management does not alter the current value and refreshes the Default Gateway field with the previous value.
4. Use the arrow keys to highlight the **SAVE** command field.
5. Press ENTER. The Event Message field at the top of the screen displays “SAVED OK”.

Setting the Default Interface

To set the default interface, perform the following steps:

1. Use the arrow keys to highlight the **Default Interface** field.
2. ENTER the interface number for the Default Gateway in this field.
3. Press ENTER. If the interface entered was a valid format, the cursor returns to the beginning of the Subnet Mask field. If the entry was not valid, the Event Message field displays “PERMISSIBLE RANGE: 1...1”. Local Management does not alter the current value and refreshes the Default Interface field with the previous value.
4. Use the arrow keys to highlight the **SAVE** command field.
5. Press ENTER. The Event Message field at the top of the screen displays “SAVED OK”.

SNMP Community Names Screen

This section explains how to assign community names. Community names allow you to control Local Management access by establishing three passwords. Each password controls varying levels of access to CSX400 Local Management.

Access the SNMP Community Names screen, shown in **Figure 60**, from the Setup Menu screen by using the arrow keys to highlight the **SNMP Community Names** option and pressing ENTER. The SNMP Community Names screen displays.

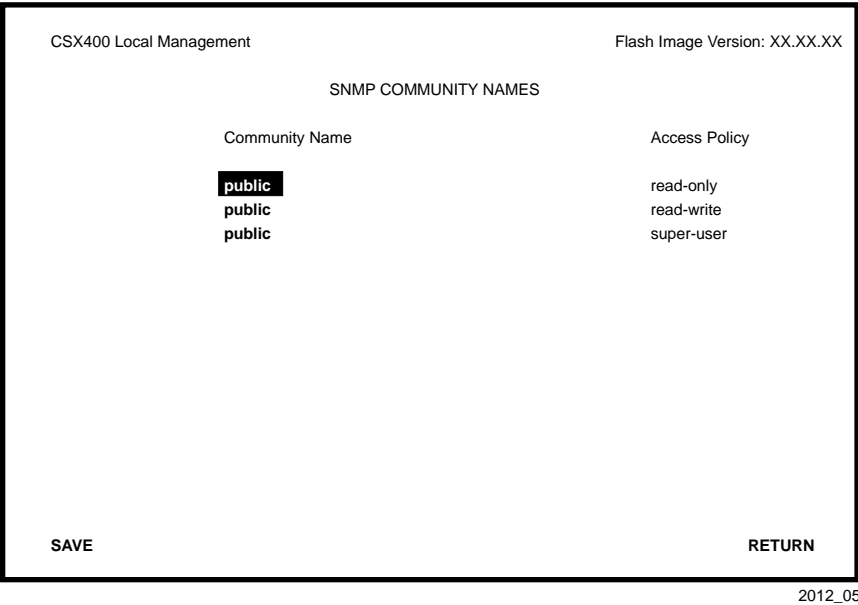


Figure 60 SNMP Community Names Screen

Community Name Access Policy

To perform any operations on the SNMP Community Names screen, you must have used the super-user community name at the User Password prompt when initiating the Local Management session. The default community name for each access level is *public* or press ENTER.

The following explains each of the SNMP Community Names screen fields:

General Configuration Using Local Management

Community Name — Displays the user-defined names through which a user accesses the CSX400 Local Management. Any community name entered here acts as a password to Local Management.

Access Policy — Indicates the access status accorded each community name. Possible status conditions are:

read-only — This access level allows reading of device parameters not including community names.

read-write — This access level allows editing of some device configuration parameters not including changing or viewing community names.

super-user — This access level allows full management privileges.

Setting SNMP Community Names

To set a community name, perform the following steps:



If you edit the super-user community name, be certain you do not forget it. If you do, you cannot perform Local Management functions without returning the device to its factory default configurations. This effectively erases any configuration work you have done.

1. Use the arrow keys to highlight the community name you want to change.
2. Type the new community name and press ENTER. The old community name is replaced by the new community name.
3. Use the arrow keys to highlight the **SAVE** command field.
4. Press ENTER. The Event Message field at the top of the screen displays “SAVED OK”.

SNMP Traps Screen

The SNMP Traps screen, shown in **Figure 61**, allows the user to configure the CSX400 to send traps to as many as eight remote management workstations. SNMP traps are messages about network events and device operational statistics.

Access the SNMP Traps screen from the Setup Menu screen by using the arrow keys to highlight the SNMP Traps option and pressing ENTER. The SNMP Traps screen displays.

CSX400 Local Management

Flash Image Version: XX.XX.XX

SNMP TRAPS

Trap Destination	Trap Community Name	Enable Traps
0.0.0.0	public	(NO)
0.0.0.0	public	(NO)
0.0.0.0	public	(NO)
0.0.0.0	public	(NO)
0.0.0.0	public	(NO)
0.0.0.0	public	(NO)
0.0.0.0	public	(NO)
0.0.0.0	public	(NO)

SAVE

RETURN

2012_06

Figure 61 SNMP Traps Screen

Trap Table Screen Fields

The following definitions explain each of the SNMP Traps screen fields:

- Trap Destination** — Use this field to enter the IP address of the management workstation designated to receive SNMP traps from the CSX400.
- Trap Community Name** — Use this field to enter the community name of the management workstation with the associated IP address. The community name indicates the “access level” of traps that will be forwarded to the Trap destination.

Enable Traps — Use this field to enable the transmission of SNMP traps to the management workstation.

Setting the SNMP Trap Destination

Each management workstation designated to receive SNMP traps from the CSX400 must have a valid IP address and community name. To set and enable SNMP trap destination, perform the following steps:

1. Use the arrow keys to highlight the **Trap Destination** field that you want to modify.
2. Type the IP address of the management workstation designated to receive SNMP traps from the CSX400. This address must be entered in DDN format.

For example: 134.141.25.17

3. Press ENTER. If the IP address entered was a valid format, the cursor returns to the beginning of the Trap Destination IP address field. If the entry was not valid, the Event Message field displays “INVALID IP ADDRESS OR FORMAT ENTERED”. Local Management does not alter the current value and refreshes the Trap Destination IP address field with the previous value.
4. Use the arrow keys to highlight the **Trap Community Name** field (on the same row as the Trap Destination field).
5. Type the community name of the management workstation. The community name indicates the “access level” of traps that will be forwarded to the Trap destination.
6. Press ENTER.
7. Use the arrow keys to highlight the **Enable Traps** field (on the same row as the Trap Destination and Trap Community Name you have just configured). The default setting for this field is **NO**.
8. Press the SPACE bar or BACKSPACE to set the field to **YES**.
9. Use the arrow keys to highlight the **SAVE** command field.
10. Press ENTER. The Event Message field at the top of the screen displays “SAVED OK”.
11. Repeat this procedure as necessary to set each Trap Destination.

Flash Download Screen

The Flash Download screen allows you to download a firmware image from a TFTP server to the CSX400.

Access the Flash Download screen from the Setup Menu screen by using the arrow keys to highlight the **Flash Download** option and pressing ENTER. The Flash Download screen, shown in **Figure 62**, displays.



Flash download operations require a properly named download file and a properly configured download server.

CSX400 Local ManagementFlash Image Version: XX.XX.XX

FLASH DOWNLOAD

Download Method:

[RUNTIME]

Reboot After Download:

[YES]

Last Image Server IP:

134.141.17.12

Last Image File Name:

c:/tftpboot/csx400.hex

Download Server IP:

134.141.17.12

Download File Name:

c:/tftpboot/csx400.hex

EXECUTE

RETURN

2012_07

Figure 62 Flash Download Screen

The following definitions explain each of the Flash Download screen fields.

Download Method — Use this field to select the method you wish to use to download the firmware image to the CSX400.

- **Reboot After Download** — This field displays when the **RUNTIME** Download Method is chosen. Selecting **YES** forces the CSX400 to reboot and use the new firmware image immediately. Selecting **NO** allows the CSX400 to continue using the existing firmware image without interrupting network operation.
- **Commit to Flash** — This field displays when the **BOOTPROM** Download Method is chosen. Selecting **YES** allows the CSX400 to continue using the existing firmware image without interrupting network operation and selecting **NO** allows the CSX400 to reboot and use the new firmware image immediately.
- **TFTP Gateway Server IP** — This field displays when the **BOOTPROM** Download Method is chosen. Use this field to enter the IP address of the TFTP Gateway Server.

Last Image Server IP — Displays the IP address of the last server used to download a firmware image to the CSX400.

Last Image File Name — Displays the file name of the last firmware image downloaded to the CSX400.

Download Server IP — Use this field to type in the IP address of the server from which you wish to download the firmware image.

Download File Name — Use this field to type in the file name of the firmware image you wish to download to the CSX400.

Selecting a Flash Download Method

1. Use the arrow keys to highlight the **Download Method** field.
2. Press the SPACE bar or BACKSPACE to select a flash download method.
 - If you select **RUNTIME**, the Reboot After Download field displays.
 - If you select **BOOTPROM**, the Commit to Flash field and the TFTP Gateway Server IP field display.

RUNTIME Download

If you select **RUNTIME Download**, perform the following steps:

1. Use the arrow keys to highlight the **Reboot After Download** field.
2. Press the SPACE bar or BACKSPACE to select one of the following:
 - **YES**, if you want the CSX400 to reboot and use the new firmware image immediately.
 - **NO**, if you want the CSX400 to continue using the existing firmware image without interrupting network operation. The CSX400 stores the new firmware image in flash memory. When you reset the CSX400, it boots from flash memory using the new image.
3. Use the arrow keys to highlight the **Download Server IP** field.
4. Type the IP address of the download server and press ENTER.
5. Use the arrow keys to highlight the **Download File Name** field.
6. Type the complete path and filename of the new image file to be downloaded. You must include all directories and subdirectories involved in accessing the file. Type the new entry over the previous entry. For example: c:\images\cyberswitch\11011.hex
7. Press ENTER.
8. Use the arrow keys to highlight the **EXECUTE** command located at the bottom of the Flash Download screen.
9. Press ENTER to begin the download. The CSX400 attempts to download the file using the IP address, filename, and path provided. This file is assigned to the Flash memory of the CSX400.

BOOTROM Download

If you select a **BOOTROM Download**, perform the following steps:

1. Use the arrow keys to highlight the **Commit to Flash** field.
2. Press the SPACE bar or BACKSPACE to select one of the following:
 - **YES**, if you want the CSX400 to continue using the existing firmware image without interrupting network operation. The CSX400 stores the new firmware image in flash memory. When you reset the CSX400, it boots from flash memory using the new image.
 - **NO**, if you want the CSX400 to reboot and use the new firmware image immediately.
3. Use the arrow keys to highlight the **Download Server IP** field.
4. Type the IP address of the download server and press ENTER.

5. Use the arrow keys to highlight the **Download File Name** field.
6. Type the complete path and filename of the new image file to be downloaded. You must include all directories and subdirectories involved in accessing the file. Type the new entry over the previous entry. For example: c:\images\cyberswitch\11011.hex.
7. Press ENTER.
8. Use the arrow keys to highlight the **TFTP Gateway Server IP** field.
9. Enter the IP address of the TFTP gateway server.
10. Use the arrow keys to highlight the **EXECUTE** command located at the bottom of the Flash Download screen. The CSX400 attempts to download the file using the IP address, filename, and path provided. This file is assigned to the Flash memory of the CSX400.

Bridge Setup Screen

The Bridge Setup screen enables you to select a Spanning Tree protocol and enable/disable bridge ports.

Access the Bridge Setup screen, shown in **Figure 63**, by using the arrow keys to highlight the **Bridge Setup** option and pressing ENTER. The Bridge Setup screen displays.

CSX400 Local Management Flash Image Version: XX.XX.XX

BRIDGE SETUP

SPANNING TREE PROTOCOL: [IEEE 802.1]

BRIDGE PORT ADMIN STATUS: PORT 01 --> ALL PORTS [ENABLED]

BRIDGE PORT PAIR ADMIN STATUS: PORT XX --> PORT [02] [ENABLED]

SAVE BRIDGE_PORT [01] RETURN

2012_08

Figure 63 Bridge Setup Screen

Bridge Setup Screen Fields

The following list describes each of the Bridge Setup screen fields:

Spanning Tree Protocol — Use this field to select a Spanning Tree protocol. Possible selections for this field are IEEE 802.1, DEC, or NONE.

Bridge Port Admin Status — Use this field to enable or disable individual CSX400 bridge ports. Possible selections for this field are ENABLED or DISABLED.

Bridge Port Pair Admin Status — Use this field to enable or disable bridging between bridge port pairs. For example, you can enable Port 1 to bridge traffic to all ports except Port 2.

Bridge_Port X — Use this command field to select the CSX400 bridge port you want to configure.

Selecting a Spanning Tree Protocol

To select the Spanning Tree protocol to be used by the CSX400, perform the following steps:

1. Use the arrow keys to highlight the **SPANNING TREE PROTOCOL** field.
2. Press the SPACE bar or BACKSPACE to select **[IEEE 802.1]**, **[DEC]**, or **[NONE]**.
3. Use the arrow keys to highlight the **SAVE** command field.
4. Press ENTER. The Event Message field at the top of the screen displays “SAVED OK”.

Selecting the Bridge Port Administrative Status

To select the bridge port administrative status, perform the following steps:

1. Use the arrow keys to highlight the **[BRIDGE_PORT XX]** field at the bottom of the Bridge Setup screen.
2. Press the SPACE bar or BACKSPACE to select the bridge port you want to configure. The selected bridge port displays in the Bridge Port Admin Status field.
3. Use the arrow keys to highlight the **BRIDGE PORT ADMIN STATUS: PORT X - - > ALL PORTS [ENABLED]** field.
4. Press the SPACE bar or BACKSPACE to select **ENABLE** or **DISABLE**.

For example, the following bridge setup indicates that bridge port 01 is configured to bridge traffic to all ports:

BRIDGE PORT ADMIN STATUS: PORT **01** - - > ALL PORTS **[ENABLED]**

5. Use the arrow keys to highlight the **SAVE** command field.
6. Press ENTER. The Event Message field at the top of the screen displays “SAVED OK”.

Selecting the Bridge Port Pair Administrative Status

To select the bridge port pair administrative status, perform the following steps:

1. Use the arrow keys to highlight the **[BRIDGE_PORT XX]** field at the bottom of the Bridge Setup screen.
2. Press the SPACE bar or BACKSPACE to select the bridge port you want to configure. The selected bridge port displays in the Bridge Port Pair Admin Status field.
3. Use the arrow keys to highlight the **BRIDGE PORT PAIR ADMIN STATUS: PORT X - -> PORT [Y]** field.
4. Press the SPACE bar or BACKSPACE to select the port you want to enable or disable bridge traffic.
5. Use the arrow keys to highlight the **BRIDGE PORT PAIR ADMIN STATUS: PORT X - -> PORT [Y] [ENABLED]** field.
6. Press the SPACE bar or BACKSPACE to select **ENABLE** or **DISABLE**.

For example, the following bridge setup indicates that bridge port 01 is configured NOT to bridge traffic to bridge port 02:

BRIDGE PORT PAIR ADMIN STATUS: PORT 01 - - > PORT [02] [DISABLED]

7. Use the arrow keys to highlight the **SAVE** command field.
8. Press ENTER. The Event Message field at the top of the screen displays “SAVED OK”.

Router Setup Screen

The Router Setup screen allows you to choose either IP or IPX routing for your CSX400.

Access the Router Setup screen, shown in **Figure 64**, by using the arrow keys to highlight the **ROUTER SETUP** menu item in the Setup Menu and pressing ENTER. The Router Setup screen displays.

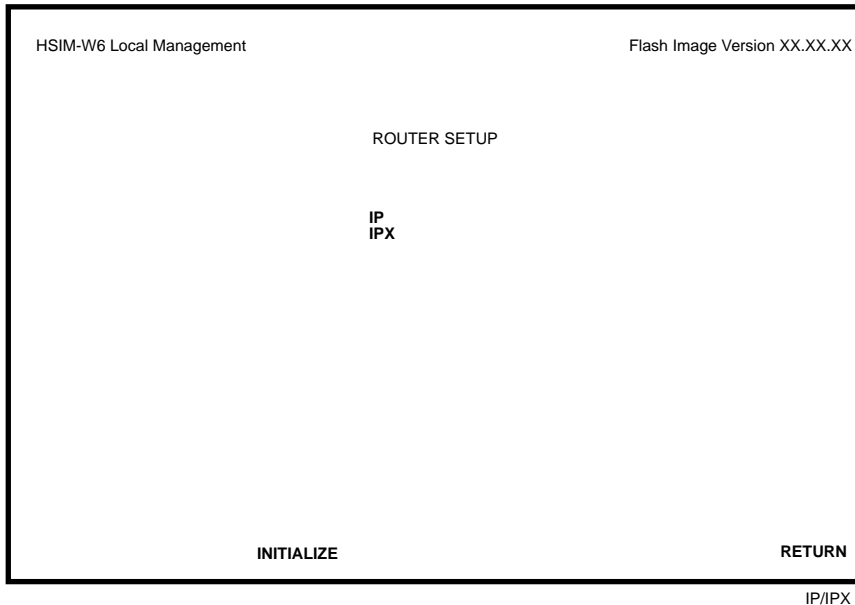


Figure 64 Router Setup Screen

Router Setup Fields

The following list describes the Router Setup fields.

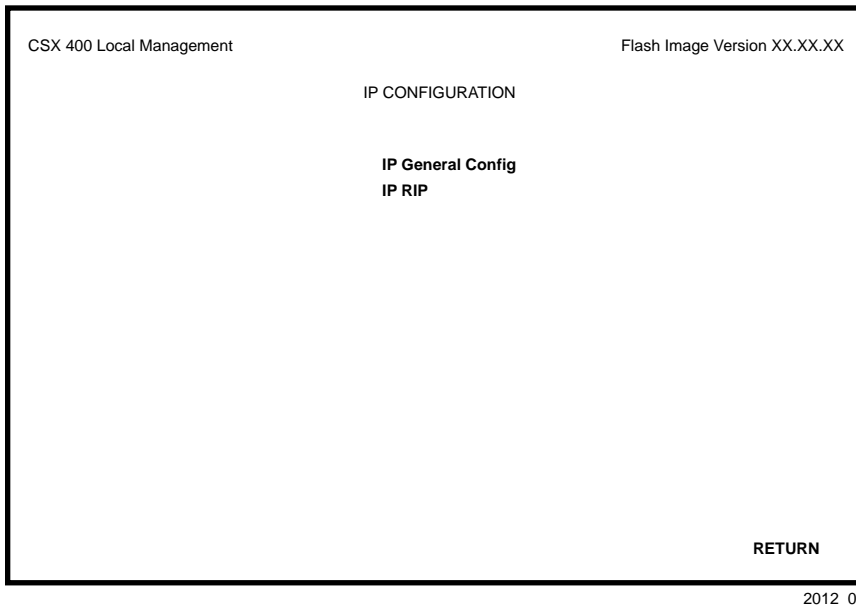
IP — Use this field to access the IP Configuration screen to configure the CSX400 for IP routing.

IPX — Use this field to access the IPX Configuration screen to configure the CSX400 for IPX routing.

IP Configuration Screen

The IP Configuration screen enables you to access the IP General Config and IP RIP screens to configure the CSX400 for IP Routing and enable RIP on the CSX400.

Access the IP Configuration screen, shown in **Figure 65**, by using the arrow keys to highlight the **IP** menu item on the Router Setup screen and pressing ENTER. The IP Configuration screen displays.



2012_09

Figure 65 IP Configuration Screen

IP Configuration Screen Fields

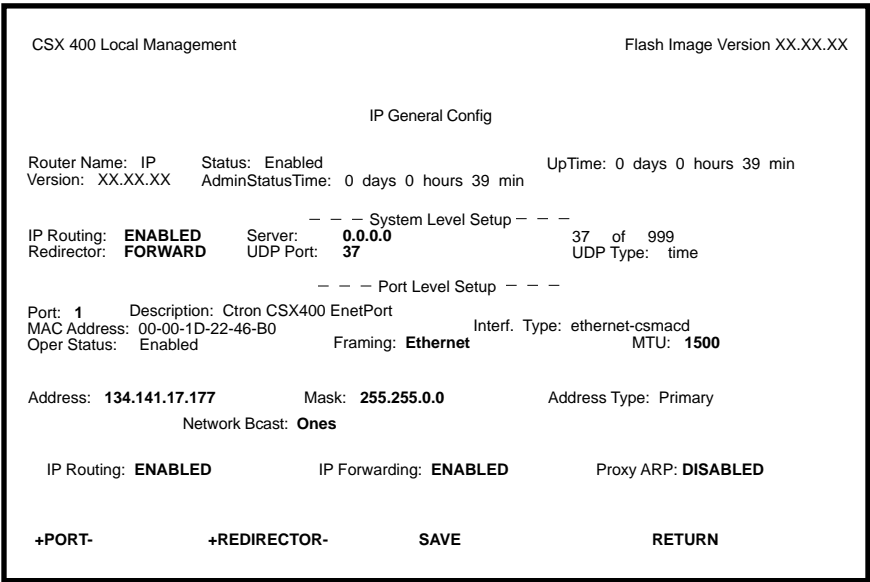
The following list describes each of the IP Configuration screen fields.

IP General Config — Use this field to access the IP General Config screen and configure the CSX400 for IP routing.

IP RIP — Use this field to access the IP RIP screen and enable Routing Information Protocol (RIP) routing on the CSX400.

IP General Config Screen

The IP General Config screen allows you to configure the CSX400 for IP routing. Access the IP General Config screen by using the arrow keys to highlight the **IP General Config** menu item and pressing ENTER. The IP General Config screen shown in **Figure 66** displays.



2012_11

Figure 66 IP General Config Screen

IP General Configuration Status Fields

The following list describes each of the IP General Config status fields. The status fields are for informational purposes only and cannot be modified.

- Router Name** — Displays the type of routing used.
- Status** — Displays the status of IP Routing.
- UpTime** — Displays the amount of time elapsed since the last time the CSX400 was rebooted.
- Version** — Displays the IP Routing version number used on the CSX400.

AdminStatusTime — Displays the amount of time elapsed since an IP address was assigned to the CSX400.

UDP Type — Displays the User Datagram Protocol (UDP) Service to which the selected UDP Port number corresponds.

Description — Describes the selected Port.

MAC Address — Displays the physical (MAC) address of the CSX400.

Interf. Type — Displays the type of interface used by the specified port.

Oper Status — Displays the operational status of the selected port.

IP General Configuration Fields

This section provides a general overview of the procedures required to configure the CSX400. The following list describes each of the modifiable IP General Config Screen fields.

+PORT- — Use this field to select the routing port you wish to configure.

+REDIRECTOR- — Use this field to toggle through a list of commonly used UDP port numbers. UDP port numbers are associated with the relay agent functionality of the router.

Framing — Use this field to select the format of the frame in which IP packets are encapsulated for transmission.

MTU — Use this field to set the Maximum Transmission Unit (MTU).

IP Routing — Use this field to enable IP Routing Services.

IP Forwarding — Use this field to enable IP Forwarding.

Proxy ARP — Use this field to enable Proxy Address Resolution Protocol (ARP).

Address — Use this field to assign an IP address to the port that you wish to configure.

Mask — Use this field to set the Subnet Mask for the port that you wish to configure.

Selecting a Port for Configuration

Routing Services allows you to choose the ports that you want to configure for IP routing. To select a router port to configure for IP routing, complete the following steps:

1. Use the arrow keys to highlight the **PORT** option.
2. Type in the number of the port that you want to configure for IP routing and then press ENTER.



You can type in the port number, or you can use the **+PORT-** option at the bottom of the screen to scroll through the list of the ports on your device. To use the **+PORT-** option, use the arrow keys to highlight the + (to go forward), or the - (to go backward), and then press **ENTER** to scroll through the available ports in the direction you have selected. You can also use the **+** and **-** keys to scroll through the available ports.

If you type in an invalid port number, the error message “PORT NUMBER IS OUT OF RANGE” displays. Perform steps 1 and 2 again.

Entering the IP Address and Subnet Mask

All IP hosts must have an IP Address for each network interface. These addresses identify each network connection.

To enter the IP address for a router port, complete the following steps:

1. Use the arrow keys to highlight the **ADDRESS** option.
2. Type in the IP address and then press ENTER.

Once an IP address is entered, the default Subnet Mask automatically enters into the Mask field. To change the default Subnet Mask for a router port, complete the following steps:

1. Use the arrow keys to highlight the **MASK** option.
2. Type in the Subnet Mask for the IP address that you have assigned.

Selecting the Frame Type for a Port

On each port, Frame Type specifies the format of the frame in which IP packets are encapsulated for transmission. The Frame Type options available for each router port are dependent on the type of media supported by that router port.

To select the Frame Type for a port, complete the following steps:

1. Use the arrow keys to highlight the **Framing** option.
2. Use the ENTER key to toggle the entry to the correct Frame Type for the port.

3. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen and then press ENTER. The message “SAVED OK” displays.

Setting the Maximum Transmission Unit (MTU)

The Maximum Transmission Unit specifies the maximum packet size for all IP packets that are transmitted.

To select the MTU for a port, complete the following steps:

1. Use the arrow keys to highlight the **MTU** option under Port Level Setup.
2. ENTER an MTU value for the media used.
3. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen, then press ENTER. The message “SAVED OK” displays.

Enabling IP Routing Services on a Port

The ability to switch IP Routing Services on and off on a port-by-port basis, provides great flexibility. On the same device, some ports can be routing IP traffic while other ports are bridging it. As you are in transition from a bridged network to a routed network, this flexibility allows you to implement IP routing and test your routing configuration on a port-by-port basis. If necessary, you can temporarily disable the IP routing on any port without losing your configuration, or you can temporarily switch from IP routing back to bridging.

To enable IP Routing Services on a router port, complete the following steps:

1. Use the arrow keys to highlight the **IP Routing** option under Port Level Setup.
2. Use the ENTER key to toggle the entry to **ENABLED**.
3. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen, and then press ENTER. The message “SAVED OK” displays.

Enabling IP Forwarding on a Port

By default, IP Forwarding is disabled on each router port. Your device cannot begin forwarding IP data packets on any router port until you enable IP Forwarding on that port.

To enable IP Forwarding on a router port, complete the following steps:

1. Use the arrow keys to highlight the **IP Forwarding** option.
2. Use the ENTER key to toggle the entry to **ENABLED**.

3. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen and then press ENTER. The message “SAVED OK” displays.

Configuring the UDP Broadcast Redirector

To locate a server that can provide a particular network service, many IP hosts rely on the use of LAN broadcasts to send UDP service requests. The UDP port number contained in the broadcast request packet identifies the service being requested. **Table 23** shows the port numbers and their corresponding requested services.

Table 23 UDP Port Numbers

UDP Port #	UDP Services
37	Time
42	Host Name Server
53	Domain Name Server
65	TACACS-Database Service
67	Bootstrap Protocol/Dynamic Host Control Protocol Server
68	Bootstrap Protocol/Dynamic Host Control Protocol Client
69	Trivial File Transfer
137	NETBIOS Name Server
138	NETBIOS Datagram Server
111	Sunrpc (NIS)

The UDP Broadcast Redirector enables you to configure any Routing Services enabled device to forward the UDP packets that it receives as LAN broadcasts, directly to the appropriate server. UDP service requests that are sent as LAN broadcasts by clients of applications such as Host Name, Domain Name, and Bootstrap servers, can be redirected to any server on any network segment.

To configure the UDP Broadcast Redirector, complete the following steps:

1. Use the arrow keys to highlight the **UDP Port** option under System Level Setup.
2. ENTER the UDP port number of the UDP service request packets that you want to redirect (refer to **Table 23**) and then press ENTER.

3. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen and then press ENTER. The message “SAVED OK” displays.



You can type in the UDP port number, or you can use the **+REDIRECTOR-** option at the bottom of the screen to scroll through a list of commonly used UDP port numbers. To use the **+REDIRECTOR-** option, use the arrow keys to highlight the **+** (to go forward), or the **-** (to go backward), and then press the **ENTER** key to scroll in the direction that you selected.

The entry for the UDP Port option reflects the UDP port number that is currently selected. The entry for UDP Type names the UDP service to which that port number corresponds.

Enabling Proxy ARP on a Port

By default, Proxy Address Resolution Protocol (ARP) is disabled on all ports, and IP Routing Services respond only to ARP requests addressed to its own IP address.

For one IP host to communicate with another IP host, knowledge of the target host's MAC address must be known. To learn this MAC address, the IP host sends an ARP request packet as a LAN broadcast with the destination IP address of the target IP host. All hosts receive this broadcast and the one host that matches the target IP address responds with its MAC-layer address. However, because each subnet constitutes a separate broadcast domain and LAN broadcasts are not forwarded across routers, ARP does not work beyond a host's local network or subnetwork. One of the primary purposes of a router is to confine LAN broadcast traffic to each local network or subnetwork.

A proxy ARP response is generated when the following occurs:

- Proxy ARP is enabled on a router port.
- An ARP request is received as a LAN broadcast (looking for the MAC-layer address of an IP host on another network segment).
- An entry exists in the IP Forwarding Table for the destination host's network.

Enabling Proxy ARP on a router port allows IP hosts to dynamically obtain the MAC-layer address of other IP hosts attached to different networks or subnetworks by using broadcast ARP request packets. With Proxy ARP enabled, IP hosts are not required to maintain knowledge of specific subnetworks.

To enable Proxy ARP on a router port, complete the following steps:

1. Use the arrow keys to highlight the **Proxy ARP** option.
2. Use the ENTER key to toggle the entry to **ENABLED**.

3. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen, and then press ENTER. The message “SAVED OK” displays.

Configuring the Network Broadcast Type on a Port

IP Routing Services recognizes and accepts network broadcasts, IP packets with the host portion of the IP address as either all 1's or all 0's. Other networking devices only recognize all 0's as a network broadcast.

To configure IP Routing Services to send network broadcasts addressed to all 0's, complete the following steps:

1. Use the arrow keys to highlight the **Network Bcast** option.
2. Use the ENTER key to toggle the entry to **ZEROS**.
3. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen and then press ENTER. The message “SAVED OK” displays.

Enabling the RIP Routing Protocol on a Port

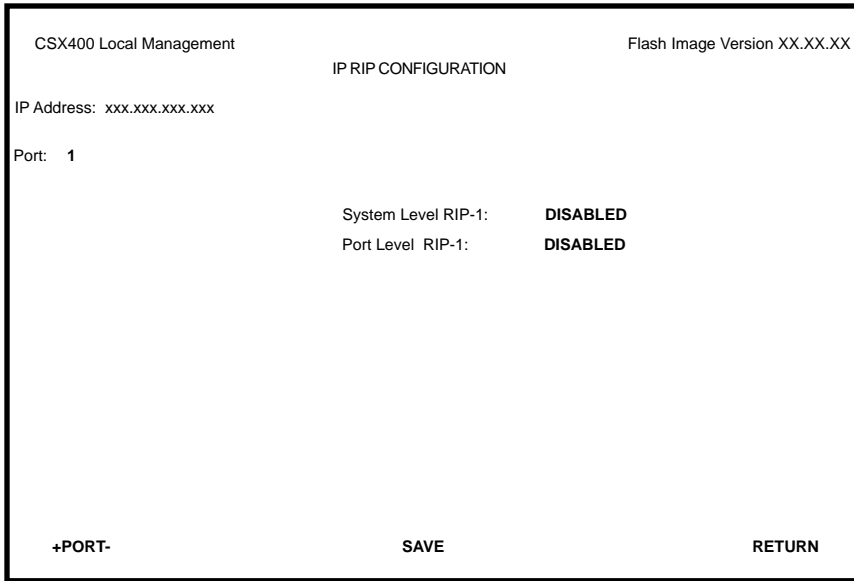
Routing Information Protocol (RIP) is a widely implemented routing protocol that is used extensively on IP internetworks. IP Routing Services uses the RIP routing protocol to send and gather information about the internetwork topology. This information is used to construct and maintain a database called RIP Route Table, which contains the addresses of the available routes to all the networks and hosts that RIP has learned.

Enabling the RIP routing protocol allows IP Routing Services to build and maintain a dynamic database of route information. The best routes learned by the RIP routing protocol are added to the IP Forwarding Table to forward IP packets. The ability to switch the RIP routing protocol on and off on a port-by-port basis provides great flexibility. On the same device, some router ports can be running the RIP routing protocol while other router ports are not. If necessary, you can temporarily disable the RIP routing protocol on any port without affecting the rest of your configuration.

To enable RIP Routing, complete the following steps:

1. From the IP Configuration screen, highlight **IP RIP** and then press ENTER.
The IP RIP Configuration screen, shown in **Figure 67**, displays.
2. Use the arrow keys to highlight the **System Level RIP-1** option.
3. Use the ENTER key to toggle the entry to **ENABLED**.
4. Use the arrow keys to highlight the **Port Level RIP-1** option.

5. Use the ENTER key to toggle the entry to **ENABLED**.
6. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen, and then press ENTER. The message “SAVED OK” displays.



The image shows a terminal window titled "CSX400 Local Management" with a subtitle "IP RIP CONFIGURATION". The top right corner displays "Flash Image Version XX.XX.XX". The main content area shows "IP Address: xxx.xxx.xxx.xxx" and "Port: 1". Below this, there are two status lines: "System Level RIP-1: DISABLED" and "Port Level RIP-1: DISABLED". At the bottom of the screen, there are three navigation options: "+PORT-", "SAVE", and "RETURN".

```
CSX400 Local Management                               Flash Image Version XX.XX.XX
IP RIP CONFIGURATION
IP Address: xxx.xxx.xxx.xxx
Port: 1
System Level RIP-1:  DISABLED
Port Level RIP-1:    DISABLED
+PORT-                SAVE                RETURN
```

Figure 67 IP RIP Configuration Screen

IPX Configuration Screen

The IPX Configuration screen enables you to access the IPX General Config, IPX RIP, and IPX SAP screens to configure the CSX400 for IPX Routing and enable RIP routing or Source Advertisement Protocol (SAP) routing on the CSX400.

Access the IPX Configuration screen, shown in **Figure 68**, by using the arrow keys to highlight the **IPX** menu item on the Router Setup and pressing ENTER. The IPX Configuration screen displays.

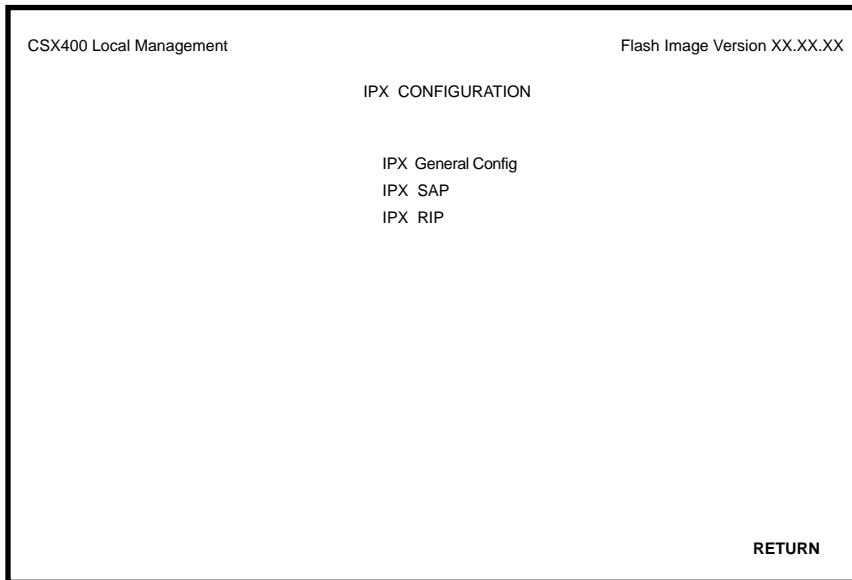


Figure 68 IPX Configuration Screen

IPX Configuration Fields

The following list describes each of the IPX Configuration screen fields.

IPX General Config — Use this field to access the IPX General Config screen and configure the CSX400 for IP routing.

IPX SAP — Use this field to access the IPX SAP screen and enable Source Advertisement Protocol (SAP) routing on the CSX400.

IPX RIP — Use this field to access the IPX RIP screen and enable Routing Information Protocol (RIP) on the CSX400.

IPX General Configuration Screen

The IPX General Configuration screen allows you to configure the CSX400 for IPX routing.

Access the IPX General Configuration screen by using the arrow keys to highlight the **IPX General Config** menu item and pressing ENTER. The IPX General Configuration screen shown in **Figure 69** displays.

CSX400 Local Management

Flash Image Version XX.XX.XX

IPX General Configuration

Router Name: IPX
Version: XX.XX.XX

Status: Enabled
AdminStatusTime: 0 days 0 hours 39 min

UpTime: 0 days 0 hours 39 min

-- -- System Level Setup -- --

IPX Routing: **ENABLED**

-- -- Port Level Setup -- --

Port: 1

Description: Ctron CSX400 EnetPort

MAC Address: 00-00-1D-22-46-B0

Interf. Type: ethernet-csmacd

Oper Status: Enabled

MTU: 1500

Framing: Novell

IPX Address: 0.0.0.0

IPX Routing: **DISABLED**

IPX Forwarding: **DISABLED**

+PORT-

SAVE

RETURN

Figure 69 IPX General Configuration Screen

IPX General Configuration Status Fields

The following list describes each of the IPX General Config status fields. The status fields are for informational purposes only and cannot be modified.

Router Name — Displays the type of routing used.

Status — Displays the status of IP Routing.

UpTime — Displays the amount of time elapsed since the last time the CSX400 was rebooted.

Version — The version number of the IP Routing used on the CSX400.

AdminStatusTime — Displays the amount of time elapsed since an IP address was assigned to the CSX400.

Description — Describes the selected Port.

MAC Address — Displays the physical (MAC) address of the CSX400.

Interf. Type — Displays the type of interface used by the specified port.

Oper Status — Displays the operational status of the selected port.

IPX General Configuration Fields

This section provides a general overview of the procedures required to configure the CSX400. The following list describes each of the IPX General Config fields.

+PORT- — Use this field to select the routing port that you wish to configure.

Framing — Use this field to select the format of the Frame in which IPX packets are encapsulated for transmission.

MTU — Use this field to set the Maximum Transmission Unit (MTU).

IPX Routing — Use this field to enable IP Routing Services.

IPX Forwarding — Use this field to enable IP Forwarding.

IPX Address — Use this field to assign an IP Address to the port that you wish to configure.

Selecting a Port for Configuration

Routing Services allows you to choose the ports that you want to configure for IPX routing. To select a router port to configure for IPX routing, complete the following steps:

1. Use the arrow keys to highlight the **PORT** option.
2. Type in the number of the port that you want to configure for IPX routing, then press **ENTER**.



You can type in the port number, or you can use the **+PORT-** option at the bottom of the screen to scroll through the list of the ports on your device. To use the **+PORT-** option, use the arrow keys to highlight the + (to go forward), or the - (to go backward), and then press **ENTER** to scroll through the available ports in the direction you have selected. You can also use the + and - keys to scroll through the available ports.

If you type in an invalid port number the error message: “PORT NUMBER IS OUT OF RANGE” displays. Perform steps 1 and 2 again.

Entering the IPX Address

All IPX hosts must have an IPX Address for each network interface. These addresses identify each network connection.

To enter the IPX Address for a router port, complete the following steps:

1. Use the arrow keys to highlight the **IPX ADDRESS** option.
2. Type in the IPX Address in Dotted Decimal Notation (DDN) format and then press ENTER.

Selecting the Frame Type for a Port

On each port, Frame Type specifies the format of the frame in which IPX packets are encapsulated for transmission. The Frame Type options available for each router port are dependent on the type of media supported by that router port.

To select the Frame Type for a port, complete the following steps:

1. Use the arrow keys to highlight the **Framing** option.
2. Use the ENTER key to toggle the entry to the correct Frame Type for the port.
3. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen and then press ENTER. The message “SAVED OK” displays.

Setting the Maximum Transmission Unit (MTU)

The Maximum Transmission Unit specifies the maximum packet size for all IPX packets that are transmitted.

To select the MTU for a port, complete the following steps:

1. Use the arrow keys to highlight the **MTU** option under Port Level Setup.
2. ENTER an MTU value for the media used.
3. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen and then press ENTER. The message “SAVED OK” displays.

Enabling IPX Routing Services on a Port

The ability to switch IPX Routing Services on and off on a port-by-port basis provides great flexibility. On the same device, some ports can be routing IPX traffic while other ports are bridging it. As you are in transition from a bridged network to a routed network, this flexibility allows you to implement IPX routing and test your routing configuration on a port-by-port basis. If necessary, you can temporarily disable IPX routing on any port without losing your configuration, or you can temporarily switch from IPX routing back to bridging.

To enable IPX Routing Services on a router port, complete the following steps:

1. Use the arrow keys to highlight the **IPX Routing** option under Port Level Setup.
2. Use the ENTER key to toggle the entry to **ENABLED**.
3. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen and then press ENTER. The message “SAVED OK” displays.

Enabling IPX Forwarding on a Port

By default, IPX Forwarding is disabled on each router port. Your device cannot begin forwarding IPX data packets on any router port until you enable IPX Forwarding on that port.

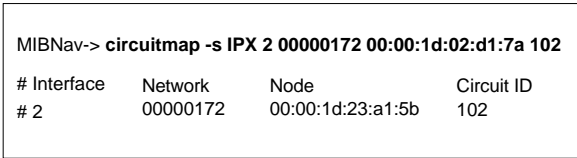
To enable IPX Forwarding on a router port, complete the following steps:

1. Use the arrow keys to highlight the **IPX Forwarding** option.
2. Use the ENTER key to toggle the entry to **ENABLED**.
3. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen and then press ENTER. The message “SAVED OK” displays.

IPX Routing over Frame Relay

An additional step is required when routing IPX over Frame Relay. This step requires that entries are created in the IPX Host Map. The IPX Host Map is a database of remote IPX hosts that are defined generally by the WAN Network number and MAC Address, and more specifically by the Interface Number and Data Link Connection Identifier (DLCI). The IPX Host Map helps a routing decision by determining which circuit a packet should be forwarded to in a point to multi-point Frame Relay connection.

Figure 70 shows how IPX Host Map entries are entered using the circuitmap command. The circuitmap command is accessed from the **MIB Navigator Screen**. Refer to **Chapter 9** for more information on the circuitmap command.

The image is a screenshot of a terminal window titled 'MIBNav->'. It shows the command 'circuitmap -s IPX 2 00000172 00:00:1d:02:d1:7a 102' being executed. Below the command, there is a table with four columns: '# Interface', 'Network', 'Node', and 'Circuit ID'. The table contains one row of data: '# 2', '00000172', '00:00:1d:23:a1:5b', and '102'.

MIBNav-> circuitmap -s IPX 2 00000172 00:00:1d:02:d1:7a 102			
# Interface	Network	Node	Circuit ID
# 2	00000172	00:00:1d:23:a1:5b	102

Figure 70 Circuitmap Command

The circuitmap command contains the following fields:

#Interface — An entry must be created for each remote Router connected via the Frame Relay interface.

Network — The Network is the IPX Network number associated with the Frame Relay network.

Node — The Node is the MAC address of the remote router on the other end of the WAN link.

Circuit ID — The Circuit ID is the DLCI identifying the virtual circuit connection to the Telco.

Enabling the IPX SAP Routing Protocol on a Port

IPX Source Advertisement Protocol (SAP) is used by IPX to exchange information about Novell service providing nodes, such as file servers and print servers that are available. IPX SAP builds and maintains a database, the Service Advertisement Table, containing the addresses and routes to specific service providing nodes, and advertises this information over the network.

Each router running IPX SAP gathers this LAN based information from the locally connected network segments and adds it to its Service Advertisement Table. Each table contains the Novell Network Number and type of services available on all Novell servers known to the IPX SAP. IPX routing services uses this information to provide internetworked NetWare clients with access to these services.

To enable SAP Routing, complete the following steps:

1. From the IPX Configuration screen, highlight **IPX SAP** and then press ENTER.
The IPX SAP Configuration screen, shown in **Figure 71**, displays.
2. Use the arrow keys to highlight the **Port** option.
3. Type in the number of the port that you wish to enable SAP routing, then press ENTER.
4. Use the arrow keys to highlight the **Port Level SAP** option.
5. Use the ENTER key to toggle the entry to **ENABLED**.
6. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen, and then press ENTER. The message “SAVED OK” displays.

```
CSX400 Local Management                               Flash Image Version XX.XX.XX
IPX SAP CONFIGURATION
IPX Address: xxx.xxx.xxx.xxx
Port: 1
System Level SAP:  DISABLED
Port Level SAP:   DISABLED
+PORT-             SAVE             RETURN
```

Figure 71 IPX SAP Configuration Screen

Enabling RIP on a Port

IPX RIP (Routing Information Protocol) is a widely implemented routing protocol that is used extensively on IPX intermediations. IPX Routing Services uses the RIP to send and gather information about the internetwork topology. This information is used to construct and maintain a database, called the RIP Route Table, containing the addresses and available routes to all the networks and hosts that RIP has learned.

Enabling RIP allows IPX Routing Services to build and maintain a dynamic database of route information. The best routes learned by RIP are added to the IPX Forwarding Table to be used to forward IPX packets. The ability to switch RIP on and off on a port-by-port basis provides great flexibility. On the same device, some router ports can be running RIP while other router ports are not. If necessary, you can temporarily disable RIP on any port without affecting the rest of your configuration.

To enable RIP Routing, complete the following steps:

1. From the IPX Configuration screen, highlight **IPX RIP** and then press ENTER.
The IPX RIP Configuration screen, shown in **Figure 72**, displays.
2. Use the arrow keys to highlight the **Port** option.
3. Type in the number of the port that you wish to enable RIP routing and then press ENTER.
4. Use the arrow keys to highlight the **Port Level RIP** option.
5. Use the ENTER key to toggle the entry to **ENABLED**.
6. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen, and then press ENTER. The message “SAVED OK” displays.

```
CSX400 Local Management                               Flash Image Version XX.XX.XX
IPX RIP CONFIGURATION
IPX Address: xxx.xxx.xxx.xxx
Port: 1
System Level RIP:  DISABLED
Port Level RIP:   DISABLED
+PORT-            SAVE            RETURN
```

Figure 72 IPX RIP Configuration Screen

WAN Setup



This section describes the HDSL WPIM. For all other WPIMs, refer to your specific WPIM(s) Local Management Guide for information on this screen.

The WAN Setup menu item accesses two screens which allow you to configure the CSX400 for a WAN Physical Interface Module (WPIM).

Access the WAN Physical Configuration screen, shown in **Figure 73**, by using the arrow keys to highlight the **WAN SETUP** menu item and pressing ENTER. The WAN Physical Configuration screen displays.

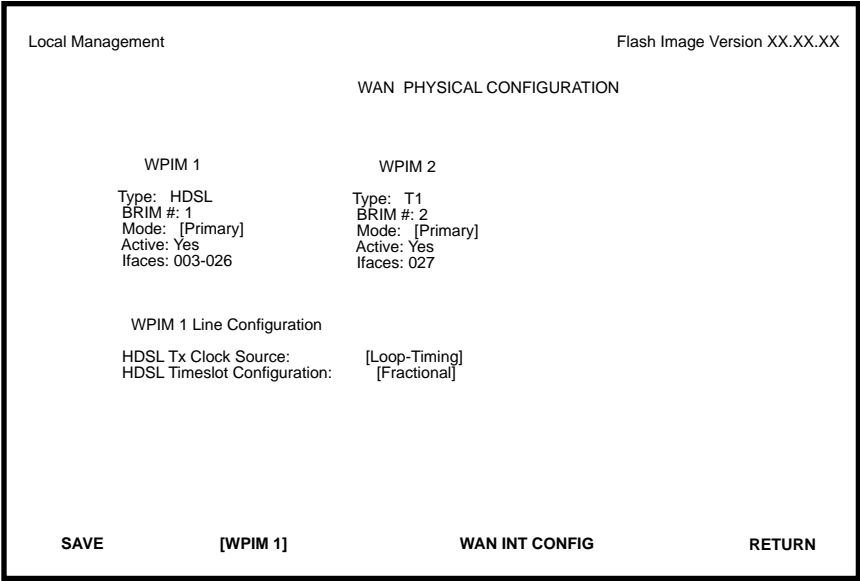
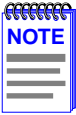


Figure 73 WAN Physical Configuration Screen

WAN Physical Configuration Screen Fields

The following list describes the WAN Physical Configuration screen fields.



The CSX400 supports a variety of WPIMs. **Figure 73** shows the WAN Physical Configuration screen for the WPIM-HDSL and the WPIM-T1. To select the WPIM you wish to configure, use the arrow keys to highlight the **[WPIM #]** field at the bottom of the screen. Use the SPACEBAR to select the appropriate WPIM, then press ENTER.

WPIM # — Displays configuration information for the WPIMs that are installed.

Type — Displays the WPIM type.

BRIM # — Displays the BRIM slot in which the WPIM resides.

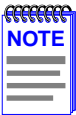
Mode — Displays the WPIM mode.

Active — Displays the status of the WPIM.

Ifaces — Displays the interfaces available to each WPIM.

WPIM-HDSL Configuration Fields

HDSL Tx Clock Source — Displays the HDSL Transmit Clock Source. The selections for this field toggle between Loop-Timing (Extracted Line Data) and Local-Timing (Internal Clock). The default setting for this field is **Loop-Timing**.



The Loop-Timing selection in this Local Management screen corresponds to the Slave selection in the QuickSET HDSL WAN Configuration window; the Local-Timing selection corresponds to the Master selection.

HDSL Timeslot Configuration — Displays the timeslot configuration for the WPIM. The selections for this field toggle between Full and Fractional. The default setting for this field is **Full**. Full uses all 24 timeslots and Fractional uses the first 12 timeslots.

WAN Interface Configuration Screen

To access the WAN Interface Configuration screen shown in **Figure 74**, use the arrow keys to highlight the **WAN INT CONFIG** selection at the bottom of the WAN Physical Configuration screen, then press ENTER.

Local Management

Flash Image Version: xx.xx.xx

WAN INTERFACE CONFIGURATION

Interface Number: [002]

Max Xmit Unit: 0

Line Coding: [NONE]

Active Protocol: [NONE]

PT#	IF#	LID	STATE	PT#	IF#	LID	STATE
001	001	Enet	UP	017			
002				018			
003				019			
004				020			
005				021			
006				022			
007				023			
008				024			
009				025			
010				026			
011				027			
012				028			
013				029			
014				030			
015				031			
016				032			

PORTS:

SAVE [xx-xxx] RETURN

1484_04

Figure 74 WAN Interface Configuration Screen

WAN Interface Configuration Screen Fields

This section describes the WAN Interface Configuration screen fields.

Interface Number — Displays the active Interface Number. Use this field to configure the Interface Numbers assigned on the WAN Physical Configuration screen.

Max Xmit Unit — User-configured field that displays the maximum packet size that can be transmitted on the selected Interface. The default values are **8191** for PPP and **4095** for Frame Relay.

Line Coding — Displays the Line Coding for Timeslots associated with this interface. This field displays JBZS, INV-HDLC, or None. The default setting is **None**.

Active Protocol — Displays the active OSI Layer protocol. This field displays None, FR (Frame Relay), or PPP (Point-to-Point). The default setting is **None**.

If you select **PPP**, the following field appears:

PPP Type: This field displays BNCP or LEX.

Circuit State: Toggles between Active, Inactive and Invalid.

PT# — Displays the application ports (bridge ports) available from the host platform to the WAN. If the active protocol is PPP, Local Management assigns only one application port per interface number (IF#). If the active protocol is Frame Relay, Local Management assigns the available WAN bridge ports from the host platform, one per DLCI.

You can assign WAN application ports to the 31 interfaces for the PPP configuration that suits your needs. In a Frame Relay configuration, you can assign all WAN application ports to one interface. In this example, the remaining 30 interfaces would not have WAN application ports available.

The quantity of application ports for a Frame Relay network is determined by the quantity of DLCIs (Data Link Connection Identifiers) assigned to that Interface. This is determined either manually or by the LMP (Link Management Protocol).

IF# — Displays the Interface that is associated with the application port.

LID — Displays the Link Identifier. If the active protocol is Frame Relay, the Data Link Connection Identifier is displayed. If the active protocol for this interface is PPP, then PPP displays in this field.

STATE — Displays the status of the application port. If the active protocol is Frame Relay, this field displays the status as Active, Inactive, or Disabled (for No LMI). If the active protocol is PPP, this field displays UP (for active) or DOWN (for inactive).

PORTS: [xx-xxx] — Toggles through the ports.

9

MIB Navigator

This chapter explains how to use the MIB Navigator utility. The MIB Navigator allows access to a command set from which you can configure and manage the CSX400.

Chapter Organization

The following list summarizes the organization of this chapter:

MIB Navigator Screen – describes the MIB Navigator screen and explains how to access it.

MIB Navigator Command Set Overview – describes the types of commands available to the MIB Navigator.

Navigation Commands – explains the commands used to navigate through the MIB Navigator.

Other Commands – explains other commands that allow you to access and manage network devices connected to the device running the MIB Navigator.

Special Commands – explains the special commands that allow you to exit from the MIB Navigator.

MIB Navigator Screen

Access the MIB Navigator screen from the Main Menu screen using Local Management (refer to the **Accessing Local Management** section in **Chapter 8**). Using the arrow keys, highlight the **MIB NAVIGATOR** option, then press ENTER. The MIB Navigator screen shown in **Figure 75** displays.

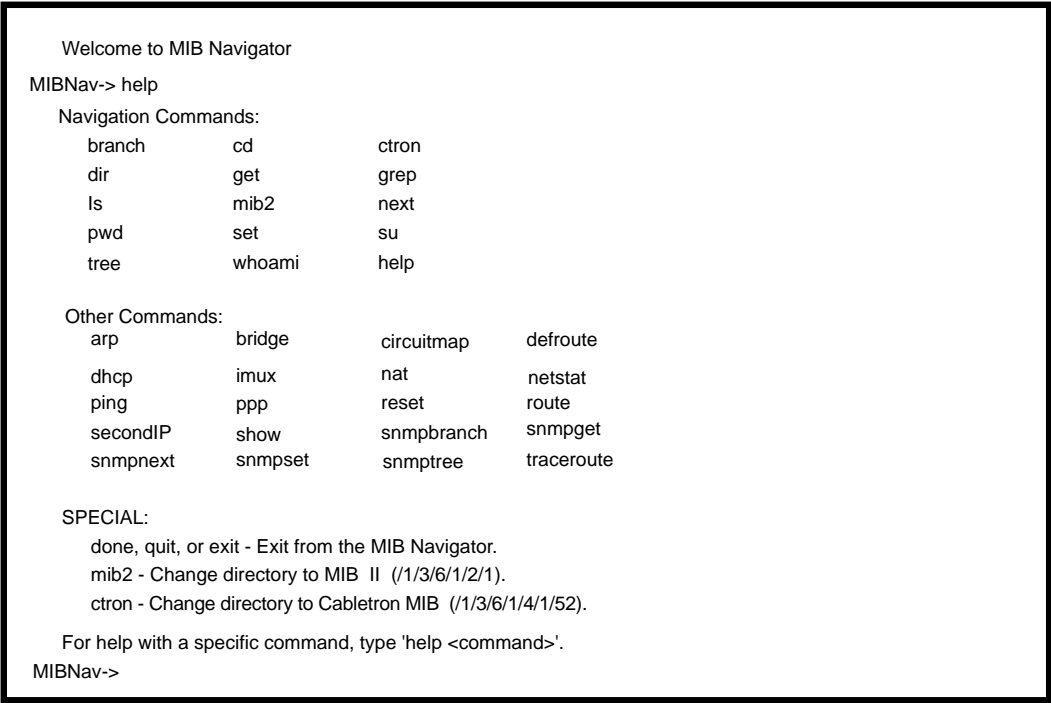


Figure 75 The MIB Navigator Screen

Managing Device MIBs

The MIB Navigator lets you manage objects in the CSX400 Management Information Bases (MIBs). MIBs are databases of objects used for managing the device and determining the CSX400 configuration. The commands within the MIB Navigator allow you to view and modify a device's objects.

The MIB Navigator views the MIB tree hierarchy as a directory. **Figure 76** shows the MIB tree hierarchy. Each layer is numerically encoded, so that every branch group and leaf object in the MIB is identified by a corresponding number, known as an Object Identifier (OID). This allows the MIB Navigator to navigate through the MIB and access the manageable leaf objects.

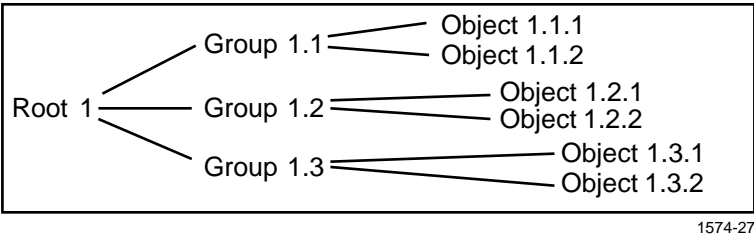


Figure 76 Hierarchical MIB Tree Structure

Often an ASCII name is assigned to the OID of a leaf object, making it more readable. To identify the value for the object “ipForwarding” you use the OID (/1/3/6/1/2/1/4/1), or its ASCII name (/iso/org/dod/internet/mgmt/mib-2/ip/ipForwarding).

MIB Navigator Command Set Overview



Use the help command for an on-line description of each MIB Navigator command. For example **MIB Nav-> help branch** provides help information for the branch command.

The MIB Navigator command set provides the following commands:

Navigation Commands — Navigation commands allow you to access and manage the MIB for the device running the MIB Navigator. Some of these commands also provide user community-string information. The commands are as follows:

branch	cd	ctron
dir	get	grep
ls	mib2	next
pwd	set	su
tree	whoami	help

Other Commands — Other commands allow you to access and manage network devices connected to the device running the MIB Navigator. The commands are as follows:

arp	bridge	circuitmap	defroute
dhcp	imux	nat	netstat
ping	ppp	reset	route
secondIP	show	snmpbranch	snmpget
snmpnext	snmpset	snmp tree	traceroute

Special Commands — Special Commands allow you to exit from the MIB Navigator. The commands are as follows:

done	quit	exit
------	------	------

Conventions for MIB Navigator Commands

This manual uses the following conventions for denoting commands:

- Information keyed by the user is shown in this helvetica font.
- Command arguments are indicated by two types of brackets:
 - required arguments are enclosed by [].
 - optional arguments are enclosed by < >.

MIB Navigator command conventions are as follows:

- To abort the output or interrupt a process the escape character is ^C (where ^ indicates the Control key).
- A slash (/) preceding an OID issues that command from the root directory regardless of where you are in the MIB. If no slash precedes the OID the command issues from your current MIB location.
- Dot notation (1.1.1.1) is equivalent to slash notation (1/1/1/1). Use slash notation with the navigational commands, and the dot notation with the built-in commands that are using SNMP to access and manage network devices.

MIB Navigation Commands are listed in the format shown below:

command:

- Syntax:** This entry provides the format that the MIB Navigator command requires. It indicates where arguments, if any, must be specified.
- Description:** This entry briefly describes the command and its uses.
- Options:** This entry lists any additional fields which may be added to the command and their format.
- Example:** This entry shows an example of the command.

Navigation Commands

The following MIB Navigation commands allow you to move from MIB object to MIB object within the MIB tree.

branch:

- Syntax:** branch [path]
- Description:** The branch command displays all of the leaves in the MIB tree below a specified path. The information displayed includes the pathname, the object ASCII name, the type of object (i.e., integer, counter, time tick, etc.), and the current value of each leaf object.
- Options:** Not Applicable
- Example:**

```
MIBNav-> branch

# /1/3/6/1/2/1/7/1  udpInDatagrams  COUNTER  38216
# /1/3/6/1/2/1/7/2  udpNoPorts      COUNTER  0
# /1/3/6/1/2/1/7/3  udpInErrors     COUNTER  0
```

051456

cd:

Syntax: cd [path] or cd <option>

Description: The cd command allows you to change directories within a MIB subtree (branch). The path specified must be valid, or the MIB Navigator will not perform the cd operation.

Options: .. Moves you one subtree above the current one.
/ Moves you to the root.

Example:

```
MIBNav-> cd iso/org/dod/internet/mgmt
```

051457

ctron:

Syntax: ctron

Description: The ctron command allows you to change directories to the Cabletron MIB (1.3.6.1.4.1.52) without keying in the entire path.

Options: Not Applicable

Example:

```
MIBNav-> ctron
```

051458

help:

Syntax: help <command>

Description: The help command provides general help on how to use the MIB Navigator or how to use a particular MIB Navigator command.

Options: A particular MIB Navigator command.

Example:

```
MIBNav-> help su
```

```
Command:      su
```

```
Format:       su <Community Name>
```

```
Allows user to change his/her community name, in  
order to allow different access to the MIB.
```

051459

mib2:

Syntax: mib2

Description: The mib2 command allows you to move directly to the MIB II subtree (1.3.6.1.2.1) without entering the entire path.

Options: Not Applicable

Example:

```
MIBNav-> mib2
```

051460

next:

- Syntax:** next [path]
- Description:** The next command enables you to determine the next leaf in the specified path within the managed device’s MIB.
- Options:** Not Applicable
- Example:**

```
MIBNav-> next /1/3/6/1/2/1

#1/3/6/1/2/1/1/1    sysDescr    String  CtronRev.X.XX.XX
```

051461

pwd:

- Syntax:** pwd
- Description:** The pwd command displays the full pathname for the directory in which you are currently working. The directory is displayed in ASCII format.
- Options:** Not Applicable
- Example:**

```
MIBNav-> pwd

# /iso/org/dod/internet/mgmt/mib-2
```

051462

set:

Syntax: set <OID> <value>

Description: The set command enables you to set the value of a managed object. This command is valid only for leaf entries in the current MIB tree, or for managed objects in the MIB.

If the leaf specified does not exist for the given path, MIB Navigator asks for a value. The following lists possible value types:

- (i)nteger - number
- (c)ounter - number
- (g)auge - number
- (t)ime ticks - number
- o(p)aque - "value" (with quotation marks)
- (s)tring - "value" (with quotation marks)
- (o)id - OID number with dotted punctuation
- (a)ddress - IP address in DDN format
- (m)ac - MAC address in hexadecimal format
- (n)ull - no type

Options: Not Applicable

Example:

```
MIBNav-> set /1/3/6/1/4/1/52/1/6/4/7 122.1.1.1
```

```
Type: (i)nteger (a)ddress (c)ounter (g)auge (o)id:
```

051463

su:

- Syntax:

su [community name]
- Description:

The su command enables you to change your community name to allow for different access to the MIB. The community name that you enter allows you either read-only, read-write, or super-user access to that device’s MIBs, depending on the level of security access assigned the password through the SNMP Community Names screen. Refer to the **SNMP Community Names Screen** section in **Chapter 8** for more information about community names.
- Options:

Not Applicable
- Example:

MIBNav-> su public

051464

tree:

- Syntax:

tree
- Description:

The tree command provides a display of the entire MIB for the device. Leaves and associated values are displayed in columns.
- Options:

Not Applicable
- Example:

MIBNav-> tree

# /1/3/6/1/2/1/1/1	sysDescr	STRING	EMRev X.X.X.X
# /1/3/6/1/2/1/1/2	sysObjectId	OBJECT ID	1.3.6.1.4.1.52
# /1/3/6/1/2/1/1/3	sysUpTime	TIME TICKS	8098654
# /1/3/6/1/2/1/1/4	sysContact	STRING	AlZwie/MIS

051465

whoami:

Syntax: whoami

Description: The whoami command displays your community string and access privileges to the MIB. When using the whoami command, one of these three access levels displays: read-only, read-write, and super-user.

Options: Not Applicable

Example:

```
MIBNav-> whoami

# Community Name      : super
# Access Level        : SuperUser
```

051466

grep:

Syntax: grep <option> string

Description: Allows a user to search the MIB tree for a specific character string. All leafs in the MIB tree are searched.

Options: -m: Displays on the terminal one screen at a time.
-i: Ignores case when searching for string.

Example:

```
MIBNav-> grep -i cabletron # /1/3/6/1/2/1/1/1 sysDescr String Cabletron MMAC-Plus Revision 01_01_01
```

051457

dir:

Syntax: dir [- 1pdm] [PATH]

Description: Lists the contents of the directory sub-tree specified. If no [directory-path] is specified, the contents of the current directory are displayed. The display options are:

- 1: Displays the OID value along with the ASCII name of the leaf object.
- p: Lists all the entries along with the path name of the leaf object.
- d: Lists only the directory entries in the tree.
- m: Displays one screen at a time.

Options: Not Applicable

Example:

```
MIBNav-> cd/iso/org/dod/internet
dir
mgmt
private
dir - lp
/1/3/6/1/4/iso/org/dod/internet/private
```

get:

Syntax: get <PATH>

Description: Returns the value of a managed object. This is only valid for “leaf” entries in the MIB tree (or managed objects in the MIB).

Options: Not Applicable

Example:

```
MIBNav-> get /1/3/6/1/2/1/1/1
#System name description
```

get

ls:

Syntax: ls [-l]pdm] [PATH]

Description: Lists the contents of the directory sub-tree specified. If no [directory-path is specified, the contents of the current directory are displayed. The display options are:

- l: Displays the OID value along with the ASCII name of the leaf object.
- p: Lists all the entries along with the path name of the leaf object.
- d: Lists only the directory entries in the tree.
- m: Displays one screen at a time.

Options: Not Applicable

Example:

```
MIBNav-> cd/iso/org/dod/internet
ls - lp
mgmt
private
ls - lp
/1/3/6/1/2 /iso/org/dod/internet/mgmt
/1/3/6/1/4 /iso/org/dod/internet/private
```

ls

Other Commands

The Other commands listed in this section activate functions on the LM managed device or devices being accessed through MIB Navigation.

arp:

Syntax: arp <options>

Description: The arp command provides access to the ARP (Address Resolution Protocol) cache, enabling you to view cache data, delete entries, or add a static route. Super-user access is required to delete an entry or add a static route.

Each ARP cache entry lists: the network *interface* that the device is connected to, the device's *network address* or IP address, the device's *physical address* or MAC address, and the *media type* of connection to the device. Media types are displayed as numbers, which stand for the following states:

- 1 - Other
- 2 - Invalid entry (cannot ping device, timed out, etc.)
- 3 - Dynamic route entry
- 4 - Static route entry (not subject to change)

Options:

- a Views cache data
- d Deletes an IP address entry.
Requires additional arguments: <Interface Number> <IP address>
- s Adds a static entry.
Requires additional arguments: <Interface Number> <IP address>
<MAC address>

Example:

```
MIBNav-> arp -a
# Interface      Network Address  Physical Address  Media Type
# (SonicInt)     122.144.40.111   00.00.0e.12.3c.04 3(dynamic)
# (SonicInt)     122.144.48.109   00.00.0e.f3.3d.14 3(dynamic)
# (SonicInt)     122.144.52.68    00.00.0e.12.3c.04 3(dynamic)
# (SonicInt)     122.144.21.43    00.00.0e.03.1d.3c 3(dynamic)

MIBNav-> arp -d 1 122.144.52.68

MIBNav-> arp -s 1 22.44.2.3 00:00:0e:03:1d:3c
```

0E1467

defroute:

Syntax: defroute [interface number] [IP address]

Description: The defroute command allows you to set the default IP route to a managed device through the specified interface.

Options: Not Applicable

Example:

```
MIBNav-> defroute 2 147.152.42.32
```

051469

dhcp:

Syntax: dhcp <options>

Description: The dhcp command provides a status of the Dynamic Host Configuration Protocol feature. Allows the user to enable/disable DHCP globally and by interface, and to configure interfaces with server parameters.

Options: dhcp (with no options) Displays DHCP status information.
dhcp enable/disable. Enables or disables the DHCP feature globally.
dhcp <IFNUM> enable disable Enables or disables the DHCP feature by interface.

dhcp reclaim <IPADDRESS> Reclaims an IP address so another client can use it.

dhcp <IFNUM> <GATEWAY> <DNSADDRESS> <WINSADDRESS> <DOMAINNAME> The IFNUM is the Ethernet port number. The four configuration parameters can be passed to the hosts (clients). These are the IP address of their default gateway, the IP address of their domain name server, the IP address of their WINS server, and their domain name.

dhcp <IFNUM> <NETADDRESS> <NETMASK> <LOWADDRESS> <HIGHADDRESS> <LEASE> Allows the user to specify the lease period for the hosts (clients), from one hour to many years. Selectable on a per port basis only.

<IFNUM> The Ethernet port number.

<NETADDRESS> The IP network on which the hosts will reside.

<NETMASK> The subnet mask for the hosts.

<LOWADDRESS> The lowest numerical value of the IP range to be allocated.

<HIGHADDRESS> The highest numerical value of the IP range.

Example:

MIBNav->dhcp

DHCP Server Summary:

Admin: Enabled Oper: Enabled Server Time: 458400

Discovers: 0, Offers: 0, Requests: 2, Errors: 0

Declines: 0, Releases: 0, Acks: 2, Naks: 0, Other Servers: 0

DHCP Interface Configuration:

IF	Admin	Oper	ServerIP	Active	Free
1	Enabled	Enabled	192.168.254.254	2	250

IF	Net Address	Net Mask	Low Address	High Address	Lease
1	192.168.254.0	255.255.255.0	192.168.254.2	192.168.254.253	2880

IF	Default Gateway	DNS Address	WINS Address	Domain Name
1	192.168.254.254	134.141.72.219	134.141.70.34	ctron.com

DHCP Client Status:

#	IF	MAC Address	Net Address	Time Left	Name
1	1	00:a0:c9:39:5e:40	192.168.254.2	22980	crotty
2	1	00:00:1d:16:71:99	192.168.254.3	22980	slowhand

dhcp

nat:

Syntax: nat <options>

Description: The nat command provides status relating to Network Address Translation. Allows the user to assign a private network to an interface, to define an interface to access the internet through, and to create a public IP address to be used on the internet. Allows the user to assign a host on the private network as a “proxy server” accessible from the internet.

Options: nat (with no options) displays status information
nat enable/disable Enables or disables the NAT feature.
nat config <PRIVATEIFNUM> <PUBLICIFNUM> Selects the local and public interfaces.
nat proxy add <ENTRY_NUMBER> <PRIVATEIP> <PUBLICPORT> <LOCALPORT> <PROTOCOL> Adds a proxy server
nat proxy delete <ENTRY_NUMBER> Deletes a proxy server

Example:

```
MIBNav->nat
NAT Status:
Admin: Enabled  Oper: Enabled  Local Interface: 1  Internet Interface: 2
Local IP      Local mask    Internet IP      Internet mask
192.168.254.254  255.255.255.0  134.141.17.165  255.255.0.0

Connections- TCP: 0, UDP: 0, ICMP: 0

Local to inet- pkts: 116, bytes: 10814

Inet to local- pkts: 91, bytes: 39812

Errors: cksum: 0, retries: 1, bad packets: 0

Total IP pkts: 3917, Reserved addresses: 2919

Server List:
Connections: #
# Number of valid entries: 0
```

nat

netstat:

- Syntax:

netstat <option>
- Description:

The netstat command provides a display of general network statistics for the managed device. The netstat command must be used with one of the two display options.
- Options:

-i Display status and capability information for each interface

-r Display routing information for each interface
- Example:

```
MIBNav-> netstat -i
Interface + Description      MTU      Speed      Admin  Oper  MAC Addr
# 1 (ethernet - csmacd)    1514     10000000   up     up    0x00 0x00 0x1d 0x07 0x50 0x0e
# 2 (ethernet - csmacd)    1514     10000000   up     up    0x00 0x00 0x1d 0x07 0x50 0x0f
# 3 (ethernet - csmacd)    1514     10000000   up     up    0x00 0x00 0x1d 0x07 0x50 0x10
# 4 (ethernet - csmacd)    1514     10000000   up     up    0x00 0x00 0x1d 0x07 0x50 0x11

MIBNav-> netstat -r
Destination      Next-hop      Interface
# Default Route  DirectConnection  1
# 134.141.0.0    DirectConnection  2
# 134.141.0.0    DirectConnection  3
```

051470

ping:

- Syntax:

ping [IP address]
- Description:

The ping command generates an outbound ping request to check the status (alive/not alive) of a device at a specified IP address.
- Options:

Not Applicable
- Example:

```
MIBNav-> ping 122.144.40.10

122.144.40.10 is alive
```

051471

snmpbranch:

- Syntax:

snmpbranch [IP address] [community name] [OID]
- Description:

The snmpbranch command enables you to query another SNMP device. The command provides a display of objects that match the specified OID. If no match is made, no object is displayed.
- Options:

Not Applicable
- Example:

```
MIBNav-> snmpbranch 2.4.8.1 public 1.3.6.2.1.1

# /1/3/6/1/2/1/1/1 sysDescr STRING EMRev X.X.X.X
# /1/3/6/1/2/1/1/2 sysObjectId OBJECT ID 1.3.6.1.4.1.52
# /1/3/6/1/2/1/1/3 sysUpTime TIME TICKS 8098654
# /1/3/6/1/2/1/1/4 sysContact STRING AlZwie/MIS
```

051473

snmpget:

- Syntax:

snmpget [IP address] [community name] [OID]
- Description:

The snmpget command enables you to query another SNMP device to obtain a value for a specified object. This command requires the appropriate community string and object id.
- Options:

Not Applicable
- Example:

```
MIBNav-> snmpget 22.44.61.22 public 1.3.6.1.2.1.1.1.0

# Cabletron EMME Revision X.XX.XX
```

051474

snmpset:

Syntax: snmpset [IP address] [community name]

Description: The snmpset command enables you to set the value of an object in other SNMP devices. This command requires the appropriate community string and OID.

When defining a new leaf set, MIB Navigator asks for a value. The following lists possible value types:

- (i)nteger - number
- (c)ounter - number
- (g)auge - number
- (t)ime ticks - number
- o(p)aque - "value" (with quotation marks)
- (s)tring - "value" (with quotation marks)
- (o)id - OID number with dotted punctuation
- (a)ddress - IP address in DDN format
- (m)ac - MAC address in hexadecimal format
- (n)ull - no type

Options: Not Applicable

Example:

```
MIBNav-> snmpset 122.44.1.2 public
1.3.6.1.2.1.1.4.0 "Cyrus/MIS"
```

051475

snmptree:

- Syntax:snmptree [IP address] [community name]
- Description:The snmptree command provides a display of all objects in the device and their corresponding values.
- Options:Not Applicable
- Example:

```
MIBNav-> snmptree 122.144.89.10 public

# /1/3/6/1/2/1/1/1 sysDescr STRING EMRev X.X.X.X
# /1/3/6/1/2/1/1/2 sysObjectld OBJECT ID 1.3.6.1.4.1.52
# /1/3/6/1/2/1/1/3 sysUpTime TIME TICKS 8098654
# /1/3/6/1/2/1/1/4 sysContact STRING AlZwie/MIS
```

051476

tracertoute:

- Syntax:tracertoute [IP address]
- Description:The tracertoute command generates a TRACEROUTE request to a specified IP address and provides a display of all next-hop routers in the path to the device. If the device is not reached, the command displays all next-hop routers to the point of failure.
- Options:Not Applicable
- Example:

```
MIBNav-> tracertoute 122.144.11.52

# next-hop[1] 122.144.61.45
# next-hop[2] 122.144.8.113
```

051477

bridge:

Syntax: bridge <ENABLE/DISABLE> <IFNUM/ALL>

Description: Allows management of bridging upon one or more interfaces of the device. Bridging may be enabled or disabled at your request, either one at a time or all at once. Specifying a single interface number affects the bridging status of that interface, while specifying ALL affects every interface of the device.

Options: <ENABLE/DISABLE> Enables or disables bridging.
<IFNUM/ALL> Allows you to specify an interface number.

Example:

MIBNav->

bridge disable all

bridge enable 1

bridge disable 1

bridge

circuitmap:

Syntax:

```
circuitmap -a <PROTOCOL>
circuitmap -f <PROTOCOL>
circuitmap -d <PROTOCOL> <INTERFACENUM>
<NETADDRESS> <MACADDRESS>
circuitmap -s <PROTOCOL> <INTERFACENUM>
<NETADDRESS> <MACADDRESS> <CIRCUIT>
```

Description: Allows the user to view and/or modify a Protocol’s Circuit Map (i.e., address-to-circuit) table for the device. The -a option shows the user the current Host Map information for the device. The -d option allows the user to delete an entry from the table. The -s option allows the user to insert a static entry into the table. The -f option allows the user to flush the table. The device must be initialized after changing the Circuit Map.

Options: Not Applicable

Example:

MIBNav-> **circuitmap -s IPX 2 00000172 00:00:1d:02:d1:7a 102**
MIBNav-> **circuitmap -a**

#	Interface	Network	Node	Circuit ID
# 2		5A4C212B	00:00:1d:23:a1:5b	203
# 2		00000172	00:00:1d:23:a1:5b	102

circuitmap

ppp:

Syntax: ppp

Description: Provides additional status relating to PPP and its Network Control Protocols.

Options: Not Applicable

reset:

Syntax: reset

Description: The reset command allows you to perform a soft reset of the device. The user is queried to confirm the reset command to insure against unwanted resets.

Note: The MIB Navigator's connection to the device is terminated upon execution of this command.

Options: Not Applicable

route:

Syntax: route add <IPADDRESS> <IPADDRESS> <INTERFACENUM>
route add <IPADDRESS> <IPADDRESS> <INTERFACENUM>
<METRIC>
route delete <IPADDRESS> <IPADDRESS> <INTERFACENUM>

Description: Allows you to add or delete static entries in the IP Forwarding Table for the device. The first address is the destination. The second address is the next hop for the given interface. The metric value is optional. If included, it is used to set the value of **ipForwardingMetric1**. When RIP is used, the metric specifies the distance in hops to the destination.

secondIP:

Syntax: secondIP add <IPADDRESS> <INTERFACENUM>
secondIP delete <IPADDRESS> <INTERFACENUM>

Description: Allows you to add or delete secondary IP addresses on the interface.

Options: Not Applicable

show:

Syntax: show <PROTOCOL> [TABLE]

Description: The show command displays information concerning various components of the device. Protocols currently supported are IP and IPX. Components of those protocols that are currently supported are ARP caches, route tables, FIB tables, server tables, and interface tables. The number of valid entries in the table is outputted at the end of the table display.

Example:

MIBNav-> show IP ARP			
# Interface	Media Type	Physical Address	Network Address
# 4	(dynamic)	00:00:1d:04:40:5d	203
# 4	(dynamic)	08:00:20:0e:d8:31	102

show

snmpnext:

Syntax: snmpnext [IPADDRESS] [COMMUNITY-STRING] [OBJECT-ID]

Description: The snmpnext command allows the user to query another device using SNMP. The next leaf of an object identifier can be retrieved from that device by supplying an appropriate community string and the values of the object identifier.

Options: Not Applicable

Example:

MIBNav-> snmpnext 132.111.22.33 public 1.3.6.1.2.1.1.2			
#1.3.6.1.2.1.1.1.3 sysUpTime	Time Ticks	5490075	

snmpnext

imux:

Syntax: imux <options>

Description: This function lets you balance your LAN traffic between two T1 WAN ports and is used with Point to Point Protocol (PPP). When you select Inverse Multiplexing via QuickSET, bridging, IP routing, and IPX routing functions are all disabled. The WAN device at the other end of the WAN link(s) must be a Cabletron Systems device, capable of receiving the balanced WAN traffic. The imux command with no options displays the status information.

Options:

- ea enables the Inverse Multiplexer Application.
- da disables the Inverse Multiplexer Application.
- eg <GROUPID> enables the Inverse Multiplexer group designated by <GROUPID>.
- dg <GROUPID> disables the Inverse Multiplexer group designated by <GROUPID>.
- ac <GROUPID> <INTERFACENUM> Adds the WAN channel designated by <INTERFACENUM> to the Inverse Multiplexer group designated by <GROUPID>.
- dc <GROUPID> <INTERFACENUM> Deletes the WAN channel designated by <INTERFACENUM> from the Inverse Multiplexer group designated by <GROUPID>.

<GROUPID> A unique value identifying an element in a sequence of groups which belong to the WAN Inverse Multiplexer Application.

<INTERFACENUM> The MIB II ifIndex value used to represent a WAN channel that has an appropriate datalink protocol associated with it.

Example:

MIBNav-> imux				
WAN Inverse Multiplexer Status:				
Group ID	Channel ID	WAN Physical Number	Available BW (Kbits/sec)	Xmit Byte Count (bytes)
1	1	1	1536000	291483387
1	2	2	1536000	292249652
Number of WAN Inverse Multiplexer Groups currently programmed: 1				
Number of WAN Inverse Multiplexer Channels currently programmed: 2				

imux

Special Commands

done, quit, exit:

Syntax: done

Description: These commands enable you to exit from the MIB Navigator and return to the Main Menu screen.

Options: Not Applicable

Example:

```
MIBNav-> done
```

```
Connection closed
```

051472

10 Troubleshooting

Use this chapter in conjunction with the LANVIEW status monitoring and diagnostic LEDs on the CSX400 to diagnose power failures, collisions, cable faults and link problems. **Figure 77** shows the front panel LEDs. **Table 24**, **Table 25**, **Table 26**, **Table 27**, and **Table 28** describe LED states.

If you are having difficulty installing and configuring the CSX400, perform the following steps:

- Review the *CSX400 QuickSTART Guide* to insure proper installation.
- Check that all cables and connectors have been attached properly.
- Verify that power has been applied to the CSX400.

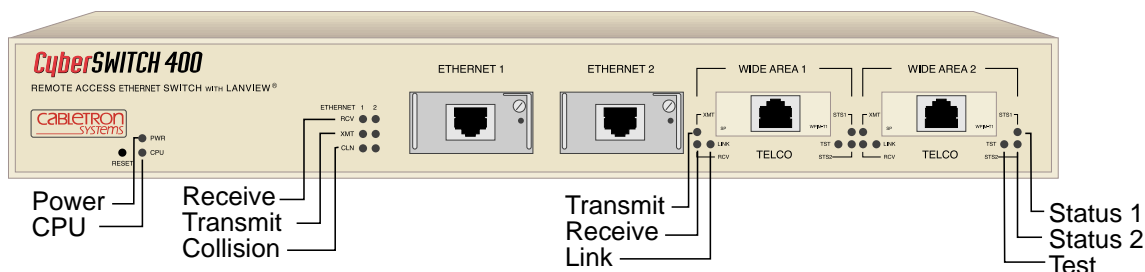


Figure 77 CSX400 Front Panel LED

Table 24 CSX400 Hardware LED States

LED	Color	State
Power (PWR)	OFF	Power off
	GREEN	Power on
Processor (CPU)	OFF	Power off
	RED	Fault condition detected
	GREEN (blinking)	NORMAL

Table 25 CSX400 LAN LED States

LED	Color	State
Receive (RCV)	OFF	Port Enabled, No Activity
	AMBER (flashing)	Receiving traffic
Collision (CLN)	OFF	NORMAL
	RED	Collision
Link (LNK)	OFF	Power Off or Failure
	GREEN	NORMAL, link exists

Table 26 CSX400 WAN LED States

LED	Color	State
Transmit (XMT)	OFF	Not transmitting traffic
	GREEN (flashing)	Transmitting traffic
Receive (RCV)	OFF	Not receiving traffic
	AMBER (flashing)	Receiving traffic
Link (LNK)	OFF	WPIM not configured
	GREEN	NORMAL, link exists
	AMBER	Link exists in STANDBY
	RED	WPIM configured, link does not exist
Test	OFF	NORMAL
	AMBER (flashing)	Power-up diagnostics Loopback testing

Table 27 CSX400 WAN LED States for STS 1

WPIM	Color	State
T1, DI, and E1	OFF	Normal or port disabled
	RED	Red alarm
DDS	OFF	Normal or port disabled
	AMBER	Out of service (OOS)
SYNC	OFF	Inactive or disabled
	GREEN	Request to send (RTS)
HDSL	OFF	Port disabled or in loopback mode
	RED	Loop 1 not synchronized, in T1 and Fractional T1 mode
	GREEN	Loop 1 synchronized
S/T	OFF	B1 not active or port disabled
	GREEN	B1 active

Table 28 CSX400 WAN LED States for STS 2

WPIM	Color	State
T1, D1, and E1	OFF	Normal or port disabled
	AMBER	Yellow alarm
DDS	OFF	Normal or port disabled
SYNC	OFF	Inactive or disabled
	GREEN	Clear to send (CTS)
HDSL	OFF	Port disabled, in Loopback mode, or Fractional T1 mode
	RED	Loop 2 not synchronized (T1 mode only)
	GREEN	Loop 2 synchronized (T1 mode only)
S/T	OFF	B2 not active or port disabled
	GREEN	B2 active

Troubleshooting CSX400 Hardware

Power (PWR) LED is OFF

- Check that the power connection is firmly attached to the back panel of the CSX400, and the other end to an active power source.

Processor (CPU) LED is OFF

If the CPU stays OFF for an extended amount of time, and the power (PWR) light remains on, the CPU is in an unknown state.

- Contact Cabletron Systems Global Call Center for technical support (refer to **Getting Help** in **Chapter 1**).

Processor (CPU) LED is RED

The processor has detected a fault condition.

- Contact Cabletron Systems Technical Support (refer to **Getting Help** in Chapter 1).

Troubleshooting the LAN

Collision (CLN) LED is RED

Collisions are normal in an Ethernet network, however, increased collisions may indicate that the network is out of specification (the propagation delay between two nodes on the network exceeds 25.6 μ s).

Link (LNK) LED is OFF

- Check that the CSX400 and the device at the other end of the segment are powered up.
- Verify that the RJ45 connectors on the twisted pair segment have the correct pinouts.
- Check the cable for continuity.
- Check that the cable meets the specifications for dB loss.

Troubleshooting the WAN

Link (LNK) LED is OFF

The WAN interface is not configured for operation.

- Use QuickSET or Local Management to make sure that the WAN interface is configured correctly.

Link (LNK) LED is RED

The WAN interface is configured, but there is no signal indicating that a valid connection is present on the WAN interface.

- Check that the CSX400 and the device at the other end of the segment are powered up.
- Use QuickSET or Local Management to make sure that both WAN interfaces, local and remote, are configured correctly.
- Check to ensure that the correct cable is being used.
- Check to ensure that the cable has continuity and is fully installed.
- Check with the WAN Service Provider to ensure that the circuit has been configured by them and is active.

Link (LNK) LED is AMBER

The port is in Standby mode.

- Check with the Network Administrator to see if management placed the port in Standby mode.
- Ensure that the protocol that you want to run has been properly selected at both ends and the time slots have been allocated if applicable.

Status 1 (STS1) LED is OFF

WPIM-T1, WPIM-E1, WPIM-DI, or WPIM-DDS Installed in CSX400

The port is operating normally. If it is not, and this LED is OFF the port may be disabled.

- Use QuickSET or Local Management to make sure that the WAN interface on the Local device is configured correctly.

WPIM-SYNC Installed in CSX400

The port is operating normally. If it is not, and this LED is OFF the port may be disabled or RTS may be inactive.

- Use QuickSET or Local Management to make sure that the WAN interface on the Local device is configured correctly.

WPIM-HDSL Installed in CSX400

The port is disabled or has been placed into Loopback Test mode.

- Use QuickSET or Local Management to make sure that the WAN interface on the Local device is configured correctly.
- Use QuickSET or Local Management to make sure that the WAN interface on the Remote device is configured correctly.

WPIM-S/T Installed in CSX400

The port is operating normally and ISDN BRI channels B1 and B2 are not active. If it is not, and this LED is always OFF, the port may be disabled.

- Use QuickSET or Local Management to make sure that the WAN interface on the Local device is configured correctly.

Status 1 (STS1) LED is RED

WPIM-T1, WPIM-E1, or WPIM-DI Installed in CSX400 is in RED Alarm Mode

A RED alarm indicates that the WAN connection is not receiving proper framing or has lost framing.

- Verify the use of proper cabling on the WAN connection.
- Check Frame Type selection on the WAN Physical Configuration and line coding.
- Possible bad cabling between Telco and CSX400.

WPIM-HDSL Installed in CSX400

WPIM-HDSL is configured for either Full or Fractional T1 and the WPIM is not able to establish synchronization on Loop 1 with the remote HDSL circuit.

- Use QuickSET or Local Management to verify that one of the WPIM-HDSLs is involved in the connection is set to Master (Local) Timing and that the other one is set to Slave (Loop) Timing.
- Verify the use of proper cabling for the HDSL connections. Category 3 or Category 5 Unshielded Twisted Pair copper wiring is required. One pair (2 wires) for Fractional T1, two pair (4 wires) for Full T1. The presence of bridged taps and multiple wire segments connected together to form the loop may reduce the maximum distance usable between the Remote and Local devices. Wire gauge has an impact on the distance which can be supported as well. The maximum distance is 12,000 feet using 24 AWG wiring.
- Verify the gauge and condition of the wire. A trained line technician may be necessary to determine this.
- Verify that the distance between the Remote and Local units is less than 12,000 Feet.

Status 1 (STS1) LED is AMBER

WPIM-DDS Installed in CSX400

The DDS circuit is Out of Service (OOS).

- Contact your WAN DDS Service Provider and have them test the operation of your DDS circuit.

Status 1 (STS1) LED is GREEN

WPIM-SYNC Installed in CSX400

The Port is operating normally; Request to Send (RTS) has been activated by your WAN device. If it is not, use the following steps:

- Use QuickSET or Local Management to make sure that the WAN interface on the local device is configured properly.
- Verify the cabling being used between the CSX400 and the CSU/DSU.

WPIM-HDSL is installed in CSX400

The Port is operating normally, Loop 1 has synchronized with the HDSL circuit at the remote end.

WPIM-S/T is installed in CSX400

The Port is operating normally, ISDN BRI channel B1 or B2 or both are active.

Status 2 (STS2) LED is OFF

WPIM-T1, WPIM-E1, WPIM-DI, or WPIM-DDS Installed in CSX400

The port is operating normally. If it is not, and this LED is OFF the port may be disabled.

- Use QuickSET or Local Management to make sure that the WAN interface on the Local device is configured correctly.

WPIM-SYNC Installed in CSX400

The port is operating normally. If it is not, and this LED is OFF the port may be disabled or CTS may be inactive from the CSU/DSU connected to the CSX400.

- Use QuickSET or Local Management to make sure that the WAN interface on the Local device is configured correctly.

WPIM-HDSL Installed in CSX400

The port is in Fractional T1 mode and is operating normally. If it is not, the port is disabled or has been placed into Loopback Test mode.

- Use QuickSET or Local Management to make sure that the WAN interface on the Local device is configured correctly.
- Use QuickSET or Local Management to make sure that the WAN interface on the Remote device is configured correctly.

WPIM-S/T Installed in CSX400

The port is operating normally and ISDN BRI channel B2 is not active. If it is not, and this LED is always OFF, the port may be disabled.

- Use QuickSET or Local Management to make sure that the WAN interface on the Local device is configured correctly.

Status 2 (STS 2) LED is RED WPIM-HDSL Installed in CSX400

WPIM-HDSL is configured for either Full T1 and the WPIM is not able to establish synchronization on Loop 2 with the remote HDSL circuit.

- Verify using QuickSET of Local Management that one of the WPIM-HDSL is involved in the connection is set to Master (Local) Timing and that the other one is set to Slave (Loop) Timing.
- Verify the use of proper cabling for the HDSL connections. Category 3 or Category 5 Unshielded Twisted Pair copper wiring is required. One pair (2 wires) for Fractional T1, two pair (4 wires) for Full T1. The presence of bridged taps and multiple wire segments connected together to form the loop may reduce the maximum distance usable between the Remote and Local devices. Wire gauge has an impact on the distance which can be supported as well. The maximum distance is 12,000 feet using 24 AWG wiring.
- Verify the gauge and condition of the wire. A trained line technician may be necessary to determine this.
- Verify that the distance between the Remote and Local units is less than 12,000 Feet.

Status 2 (STS2) LED is AMBER

WPIM-T1, WPIM-E1, or WPIM-DI Installed in CSX400

The device is in Yellow alarm mode. A Yellow alarm indicates that the CSX400 is receiving proper framing from the Telco, but the Telco is not receiving proper framing.

- Check for faulty or incorrect cabling between Telco and CSX400.
- Request that the Telco verify the configuration and operation of the circuit.

Status 2 (STS2) LED is GREEN

WPIM-SYNC Installed in CSX400

The Port is operating normally, Clear to Send (CTS) has been received by your WAN device.

- If it is not, check STS 1 to determine if the Port is Sending a Request to Send (RTS) to the CSU/DSU it is connected to.
- Verify the cabling being used between the CSX400 and the CSU/DSU.
- Check the CSU/DSU for proper operation.

WPIM-HDSL Installed in CSX400

The port is operating normally, Loop 2 has synchronized with the HDSL circuit at the remote end (Full T1 mode only).

WPIM-S/T Installed in CSX400

The port is operating normally, ISDN BRI channel B2 is active.

Test (TST) LED is AMBER (blinking)

The device is in test mode.

- The CSX400 is running its Power-up Diagnostic Tests.
- Loopback Testing is underway on a WAN circuit.

Investigating Software Configuration Problems

Software problems usually occur when your software configuration contains incomplete or incorrect information.

Connection to Device Fails During Software Configuration

- For a LAN connection, verify that the IP address matches the IP address previously stored into the configuration of the router. You must have previously (through *QuickSET*) set the Ethernet LAN IP address and Subnet Mask, enabled IP routing, saved the Ethernet configuration changes and rebooted the router for the new IP address to take effect.
- Check that your LAN cable is wired correctly and each end securely plugged in.
- Make sure that an IP route exists between your local PC and the CSX400. The PC and CSX400 must be on the same IP subnetwork or the CSX400 must be reachable through a router on your LAN.
- Check Network TCP/IP properties under Windows 95 or Windows NT, as described in the *Read Me First!* document.

User Cannot Communicate with Remote Network Station

If Bridging,

- Check that the Bridging Default Destination is set.
- Check that bridging to/from the remote router is set on.
- Be sure to reboot if you have made any bridging destination or control changes.

If TCP/IP Routing,

- Check that TCP/IP Routing is set on and is enabled at the remote end.
- Check that the IP address of the LAN beyond the remote router is correct, as well as the associated Subnet Mask.
- If the remote router WAN IP address and Subnet Mask are required, check that they have been specified correctly.
- Check that, if required, the source and remote WAN IP addresses are on the subnetwork.
- Check that you have seeded the routing table, if RIP is not allowed to flow on the WAN link.
- Be sure to reboot if you have made any IP address, control or protocol option changes.

A

EPIM Specifications

Introduction

The CSX400 provides two ports for Cabletron Systems EPIMs. EPIMs allow connection to the main network using different media types. The following sections explain the specifications of the variety of EPIMs Cabletron Systems offers.

EPIM-T

The EPIM-T is an RJ45 connector supporting UTP cabling. It has an internal Cabletron Systems TPT-T 10BASE-T Twisted Pair Transceiver.

The slide switch on the EPIM-T determines the crossover status of the cable pairs. If the switch is on the **X** side, the pairs are internally crossed over. If the switch is on the **=** side, the pairs are not internally crossed over. **Figure 78** shows the pinouts for the EPIM-T in both crossover positions.

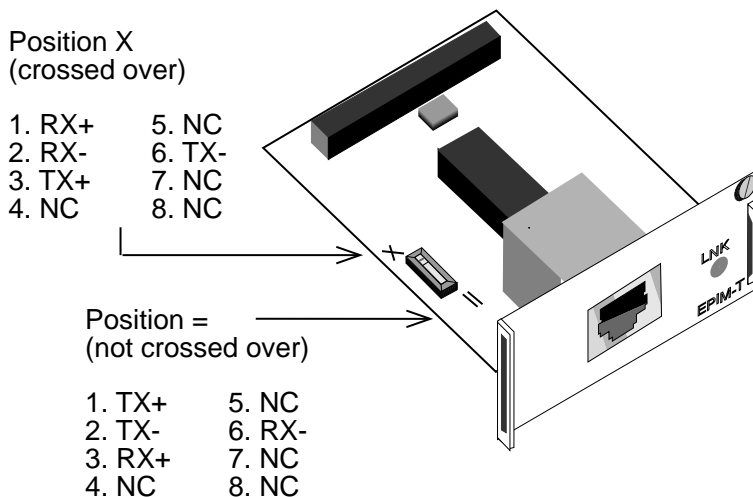


Figure 78 EPIM-T Pinouts

EPIM-F1 and EPIM-F2

The EPIM-F1 and EPIM-F2 support Multimode Fiber Optic cabling. Each EPIM has an internal Cabletron Systems FOT-F Fiber Optic Transceiver. The EPIM-F1 is equipped with SMA Connectors and the EPIM-F2 is equipped with ST Connectors. **Figure 79** shows both EPIMs. Specifications for the EPIMs are listed in **Table 29**.

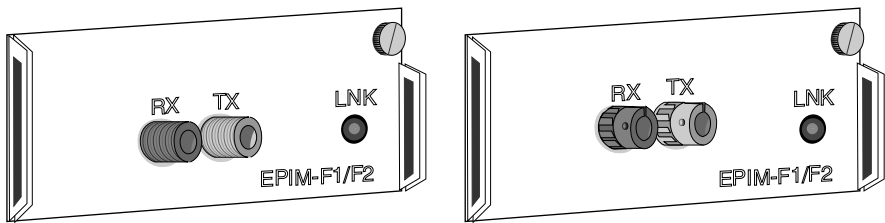


Figure 79 EPIM-F1 and EPIM-F2

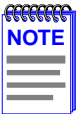
Table 29 EPIM-F1 & EPIM-F2 Specifications

Parameter	Typical Value	Worst Case
Receive Sensitivity	-30.5 dBm	-28.0 dBm
Peak Input Power	-7.6 dBm	-8.2 dBm

Table 30 provides transmitter power parameters.

Table 30 Transmitter Power

Parameter	Typical Value	Worst Case	Worst Case Budget	Typical Budget
50/125 μm fiber	-13.0 dBm	-15.0 dBm	13.0 dB	17.5 dB
62.5/125 μm fiber	-10.0 dBm	-12.0 dBm	16.0 dB	20.5 dB
100/140 μm fiber	-7.0 dBm	-9.0 dBm	19.0 dB	23.5 dB
Error Rate	Better than 10^{-10}			



The transmitter power levels and receive sensitivity levels listed are Peak Power Levels after optical overshoot. A Peak Power Meter must be used to correctly compare the values given above to those measured on any particular port. If Power Levels are being measured with an Average Power Meter, then 3 dBm must be added to the measurement to correctly compare those measured values to the values listed (i.e., -30.5 dBm peak = -33.5 dBm average).

EPIM-F3

The EPIM-F3 supports Single Mode Fiber Optic cabling. It has an internal Cabletron Systems FOT-F Fiber Optic Transceiver and is equipped with ST Connectors. **Figure 80** shows the EPIM-F3. Specifications for the EPIM-F3 are listed in **Table 31**.

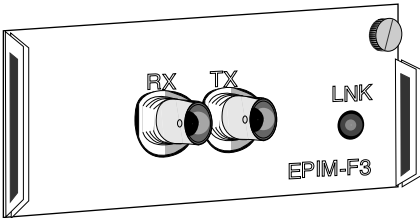
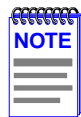


Figure 80 EPIM-F3



Transmitter Power decreases as temperatures rise and increases as temperatures fall. Use the Output Power Coefficient to calculate increased or decreased power output for your operating environment. For example, the typical power output at 25°C is -16.4 dBm. For a 4°C temperature increase, multiply the typical coefficient (-0.15 dBm) by four and add the result to typical output power (4 x -0.15 dBm + -16.4 = -17.0).

Table 31 EPIM-F3 Specifications

Parameter	Typical	Minimum	Maximum
Transmitter Peak Wave Length	1300 nm	1270 nm	1330 nm
Spectral Width	60 nm	—	100 nm
Rise Time	3.0 nsec	2.7 nsec	5.0 nsec
Fall Time	2.5 nsec	2.2 nsec	5.0 nsec
Duty Cycle	50.1%	49.6%	50.7%
Bit Error Rate	Better than 10 ⁻¹⁰		



The transmitter power levels given above are Peak Power Levels after optical overshoot. You must use a Peak Power Meter to correctly compare the values given above to those measured on any particular port. If you are measuring power levels with an Average Power Meter, add 3 dBm to the average power measurement to correctly compare the average power values measured to the values listed above (i.e., -33.5 dBm average + 3 dB = -30.5 dBm peak).

EPIM-C

The EPIM-C supports thin coaxial cabling and is equipped with an internal Cabletron Systems TMS-3 Transceiver. You can use the TERM switch on the front of the EPIM-C to set the internal 50-ohm terminator. This eliminates the need to connect the port to a T-connector and terminator.

Figure 81 shows the setting for the terminator switch.

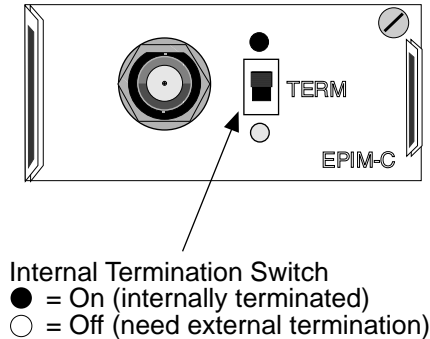


Figure 81 EPIM-C

Connector Type

This connector type is a BNC receptacle with gold center contact for use with BNC type T-connectors and RG58 coaxial cable.

Grounding



For safety reasons, only one end of a coaxial segment should be connected to earth ground. Connection to earth ground at more than one point on the segment may cause dangerous ground currents.

The BNC port of the Coaxial Interface Modules is not connected to earth ground.

EPIM-A and EPIM-X (AUI Port)

The EPIM-A is a DB15 female connector used to attach segments to an external transceiver. The EPIM-X is equipped with dual internal transceivers. It has a DB15 male connector used to attach segments to an AUI cable. **Figure 82** shows both modules and **Table 32** provides the DB15 pinouts.



The EPIM-A is equipped with a fuse (F1) to protect against risk of fire. For continued protection against the risk of fire, replace fuse F1 only with the same type and rating of fuse (1A, F250V).

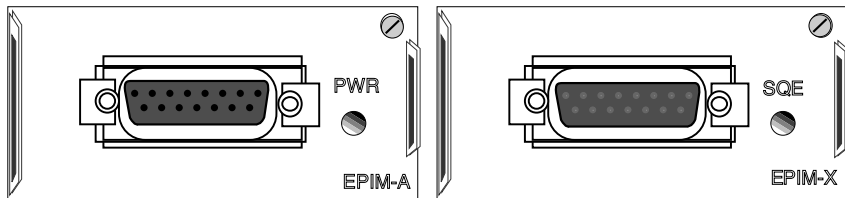


Figure 82 The EPIM-A and EPIM-X

Table 32 DB15 Pinouts

Pin Number	Represents	Pin Number	Represents
1	Logic Ref.	10	Transmit -
2	Collision +	11	Logic Ref.
3	Transmit +	12	Receive -
4	Logic Ref.	13	Power (+12Vdc)
5	Receive +	14	Logic Ref.
6	Power Return	15	No Connection
7	No Connection	Connector Shell	Positive Ground
9	Collision -		

B

WPIM Cable Specifications



For all WPIM cables, there is part number information for ordering a standard 20-foot cable or a specified length of cable. The number 20 followed by the part number denotes the standard 20-foot cable. The letter “L” denotes the specified length required in feet or meters. For example: 9372095-3 denotes a 3 foot cable; 9372095-3M denotes a 3-meter cable.

WPIM-T1

This section provides the Cabletron Systems part number and connector specifications for WPIM-T1 interface cables.

Table 33 provides connector type and part number information.

Table 33 T-1 Interface Cable Part Numbers

Connector Type	Part Number
RJ48C	9372094

Table 34 provides RJ48 connector pin assignments.

Table 34 T-1 Connector Pin Assignments

Pin	Signal
1	Receive Ring
2	Receive Tip
3	Not Used
4	Transmit Ring
5	Transmit Tip
6	Not Used
7	Shield Ground
8	Shield Ground

Table 35 provides RJ48 DTE pin assignments.

Table 35 DTE Pin Assignments

Pin	Signal
1	Receive Ring
2	Receive Tip
3	Not Used
4	Transmit Ring
5	Transmit Tip
6	Not Used
7	Shield Ground
8	Shield Ground

Table 36 provides RJ48 network pin assignments.

Table 36 Network Pin Assignments

Pin	Signal
1	Receive Ring
2	Receive Tip
3	Not Used
4	Transmit Ring
5	Transmit Tip
6	Not Used
7	Not Used
8	Not Used

WPIM-SY

This section provides the Cabletron Systems part number and connector specifications for the WPIM-SY interface cables.

Table 37 provides the cable and interface types, electrical types, and part numbers for the WPIM-SY.

Table 37 WPIM-SY Interface Cables

Cable and Interface Type	Electrical Type	Part Number
RS449	RS422	9380120
V.35	V.35	9380121
RS232	RS232	9380122
X.21	X.21	9380123
RS530	RS422	9380124
RS530 ALT A	RS422	9380125
RS530A	RS422	9380126
RS530A ALT A	RS422	9380127

EIA-449

Table 38 shows the connector number, cable assembly description, and connector type.

Table 38 EIA-449 Interface

Connector Number	Cable Assembly Description	Connector Type
1	EIA-530A ALT A to EIA-449	Sub DB 26-pin male connector
2		DB-37 pin male connector

Table 39 provides pin assignments for the EIA-449 interface cable.

Table 39 EIA-449 Interface Cable Pin Assignment

Connector 1 EIA-530A ALT A				PAIR	Connector 2 EIA-449				
MNEMONIC	DIRECT TO	NAME	PIN		PIN	NAME	DIRECT TO	MNEMONIC	
BA	DCE	Transmit Data A	2	A	4	Send Data A	DCE	SD	
		Transmit Data B	14		22	Send Data B			
BB	DTE	Receive Data A	3	B	6	Receive Data A	DTE	RD	
		Receive Data B	16		24	Receive Data B			
CB			Clear to Send A	5	C	9		Clear to Send A	CS
			Clear to Send B	13		27		Clear to Send B	
CA	DCE	Request to Send A	4	D	7	Request to Send A	DCE	RS	
		Request to Send B	19		25	Request to Send B			
DB	DTE	Transmit Signal Timing A	15	E	5	Send Timing A	DTE	ST	
		Transmit Signal Timing B	12		23	Send Timing B			
DD			Receive Signal Timing A	17	F	8		Receive Timing A	RT
			Receive Signal Timing B	9		26		Receive Timing B	
DA	DCE	Transmit Signal Timing A	24	G	17	Terminal Timing A	DCE	TT	
		Transmit Signal Timing B	11		35	Terminal Timing B			

Table 39 EIA-449 Interface Cable Pin Assignment (Continued)

Connector 1 EIA-530A ALT A				PAIR	Connector 2 EIA-449			
MNEMONIC	DIRECT TO	NAME	PIN		PIN	NAME	DIRECT TO	MNEMONIC
CE	DTE	Ring Indicator	22		15	Incoming Call	DTE	IC
TM		Test Mode	25		18	Test Mode		TM
CC		DCE Ready	6		11	Data Mode		DM
CD	DCE	DTE Ready	20		12	Terminal Ready	DCE	TR
		SHIELD	1					
AC		Signal Common	23		20	Receive Common		RC
AB		Signal Common	7		19 30 37	Send Common Terminal Ready B Signal Ground		SG TR_B SC

V.35

Table 40 shows the connector number, cable assembly description, and connector type.

Table 40 V.35 Interface

Connector Number	Cable Assembly Description	Connector Type
1	EIA-530A ALT A to V.35	Sub DB 26-pin male
2		M Series 34-pin male

Table 41 provides pin assignments for the V.35 interface cable.

Table 41 V.35 Interface Cable Pin Assignment

Connector 1 EIA-530A ALT A				PAIR	Connector 2 V.35			
MNEMONIC	DIRECT TO	NAME	PIN		PIN	NAME	DIRECT TO	MNEMONIC
BA	DCE	Transmit Data A	2	A	P	Transmit Data A	DCE	103
		Transmit Data B	14		S	Transmit Data B		
BB	DTE	Receive Data A	3	B	R	Receive Data A	DTE	104
		Receive Data B	16		T	Receive Data B		
CB		Clear to Send A	5	C	D	Ready to Send A		106
CA	DCE	Request to Send A	4	D	C	Request to Send A	DCE	105

Table 41 V.35 Interface Cable Pin Assignment (Continued)

Connector 1 EIA-530A ALT A				PAIR	Connector 2 V.35			
MNEMONIC	DIRECT TO	NAME	PIN		PIN	NAME	DIRECT TO	MNEMONIC
DB	DTE	Transmit Signal Timing A	15	E	Y	Transmitter Signal Timing A	DTE	114
		Transmit Signal Timing B	12		AA	Transmitter Signal Timing B		
DD		Receive Signal Timing A	17	F	V	Receiver Signal Timing A		115
		Receive Signal Timing B	9		X	Receiver Signal Timing B		
DA	DCE	Transmit Signal Timing A	24	G	U	Transmitter Signal Timing A	DCE	113
		Transmit Signal Timing B	11		W	Transmitter Signal Timing B		
CE	DTE	Ring Indicator	22		J	Calling Indicator	DTE	125
TM		Test Mode	25		NN	Test Indicator		142
CC		DCE Ready	6		E	Data Set Ready		107
CD	DCE	DTE Ready	20		H	Data Terminal Ready	DCE	108
RL		Remote Loopback	21		N	Loopback Maintenance		140
LL		Local Loopback	18		L	Local Loopback		141
		SHIELD	1			DRAIN		
AC		Signal Common	23		B	Signal Common		102
AB		Signal Common	7		B	Signal Common		102

EIA-232

Table 42 shows the connector number, cable assembly description, and connector type.

Table 42 EIA-232 Interface

Connector Number	Cable Assembly Description	Connector Type
1	EIA-530A ALT A to EIA-232	Sub DB 26-pin male
2		DB-25 pin male

Table 43 provides pin assignments for the EIA-232 interface cable.

Table 43 EIA-232 Interface Cable Pin Assignment

Connector 1 EIA-530A ALT A				Connector 2 EIA-232			
MNEMONIC	DIRECT TO	NAME	PIN	PIN	NAME	DIRECT TO	MNEMONIC
BA	DCE	Transmit Data	2	2	Transmit Data	DCE	BA
BB	DTE	Receive Data	3	3	Receive Data	DTE	BB
CB		Clear to Send	5	5	Clear to Send		CB
CA	DCE	Request to Send	4	4	Request to Send	DCE	CA
DB	DTE	Transmit Signal Timing	15	15	Transmitter Signal Timing	DTE	DB
DD		Receive Signal Timing	17	17	Receiver Signal Timing		DD
DA	DCE	Transmit Signal Timing	24	24	Transmitter Signal Timing	DCE	DA
CE	DTE	Ring Indicator	22	22	Ring Indicator	DTE	CE
RL	DCE	Remote Loopback	21	21	Loopback Maintenance	DCE	RL
LL		Local Loopback	18	18	Local Loopback		LL
TM	DTE	Test Mode	25	25	Test Indicator	DTE	TM
CC		DCE Ready	6	6	DCE Ready		CC
CD	DCE	DTE Ready	20	20	DTE Ready	DCE	CD
		SHIELD	1				
AC		Signal Common	23	7	Signal Common		AB
AB		Signal Common	7	7	Signal Common		AB

X.21

Table 44 shows the connector number, cable assembly description, and connector type.

Table 44 X.21 Interface

Connector Number	Cable Assembly Description	Connector Type
1	EIA-530A ALT A to X.21	Sub DB 26-pin male
2		DB-15 pin male

Table 45 provides pin assignments for the X.21 interface cable.

Table 45 X.21 Interface Cable Pin Assignment

Connector 1 EIA-530A ALT A				PAIR	Connector 2 X.21			
MNEMONIC	DIRECT TO	NAME	PIN		PIN	NAME	DIRECT TO	MNEMONIC
BA	DCE	Transmit Data A	2	A	2	Transmit A	DCE	T
		Transmit Data B	14		9	Transmit B		
BB	DTE	Receive Data A	3	B	4	Receive A	DTE	R
		Receive Data B	16		11	Receive B		
CB	DTE	Clear to Send A	5	C	5	Indication A	DTE	I
		Clear to Send B	13		12	Indication B		
CA	DCE	Request to Send A	4	D	3	Control A	DCE	C
		Request to Send B	19		10	Control B		
DB	DTE	Transmit Signal Timing A	17	E	6	Signal Element Timing A	DTE	S
		Receive Signal Timing A	15		13	Signal Element Timing B		
		Transmit Signal Timing B	9					
		Receive Signal Timing B	12					
		SHIELD	1			DRAIN		
AC		DTE Common	7		8	Signal Ground		G
AB		DCE Common	23					

EIA-530, EIA-530 ALT A, EIA-530 A, and EIA-530 A ALT A

Table 46 shows the connector number, cable assembly description, and connector type for the EIA-530, EIA-530 ALT A, EIA-530A, and EIA-530A ALT A, interface cables.

Table 46 EIA-530, EIA-530 ALT A, EIA-530A, and EIA-530A ALT A Interfaces

Connector Number	Cable Assembly Description	Connector Type
1	EIA-530A ALT A to EIA-530	Sub DB 26-pin male
2		DB 25-pin male
1	EIA-530A ALT A to EIA-530 ALT A	Sub DB 26-pin male
2		Sub DB26-pin male
1	EIA-530A ALT A to EIA-530A	Sub DB 26-pin male
2		DB 25-pin male
1	EIA-530A ALT A to EIA -530A ALT A	Sub DB 26-pin male
2		Sub DB 26-pin male

Table 47 provides the cable pin assignments for the EIA-530, EIA-530 ALT A, EIA-530A, and EIA-530A ALT A, interface cables.

Table 47 EIA-530, EIA-530 ALT A, EIA-530A, and EIA-530A ALT A Interface Cable Pin Assignments

Connector 1 EIA-530A ALT A				PAIR	Connector 2 EIA-530			
MNEMONIC	DIRECT TO	NAME	PIN		PIN	NAME	DIRECT TO	MNEMONIC
BA	DCE	Transmit Data A	2	A	2	Transmit Data A	DCE	BA
		Transmit Data B	14		14	Transmit Data B		
BB	DTE	Receive Data A	3	B	3	Receive Data A	DTE	BB
		Receive Data B	16		16	Receive Data B		
CB		Clear to Send A	5	C	5	Clear to Send A		CB
		Clear to Send B	13		13	Clear to Send B		
CA	DCE	Request to Send A	4	D	4	Request to Send A	DCE	CA
		Request to Send B	19		19	Request to Send B		

Table 47 EIA-530, EIA-530 ALT A, EIA-530A, and EIA-530A ALT A Interface Cable Pin Assignments

Connector 1 EIA-530A ALT A				PAIR	Connector 2 EIA-530			
MNEMONIC	DIRECT TO	NAME	PIN		PIN	NAME	DIRECT TO	MNEMONIC
DB	DTE	Transmit Signal Timing A	15	E	15	Transmit Signal Timing A	DTE	DB
		Transmit Signal Timing B	12		12	Transmit Signal Timing B		
DD		Receive Signal Timing A	17	F	17	Receive Signal Timing A		DD
		Receive Signal Timing B	9		9	Receive Signal Timing B		
DA	DCE	Transmit Signal Timing A	24	G	24	Transmit Signal Timing A	DCE	DA
		Transmit Signal Timing B	11		11	Transmit Signal Timing B		
RL		Remote Loopback	21		21	Remote Loopback		RL
LL		Local Loopback	18		18	Local Loopback		LL
TM	DTE	Test Mode	25		25	Test Mode	DTE	TM
CC		DCE Ready	6		6	DCE Ready		CC
CD	DCE	DTE Ready	20		20	DTE Ready	DCE	CD
SHIELD			1	DRAIN				
AC		Signal Common	23	7	Signal Common		AC	
^a AC		Signal Common	23	23	Signal Common		AC	
AB		Signal Common	7	7	Signal Common		AB	
^b CE	DTE	Ring Indicator	22	22	Ring Indicator	DTE	CE	

a. This pin assignment only applies to the EIA-530A ALT A interface cable.

b. This pin assignment only applies to the EIA-530A and EIA-530A ALT A interface cables.

WPIM-DDS

This section provides Cabletron Systems part number and connector specifications for the WPIM-DDS interface cable. The WPIM-DDS has one RJ45 port for a direct connection to a single Digital Data Service (DDS) circuit.

Table 48 provides cable and interface type, and part number information for the WPIM-DDS interface cable, and **Table 49** provides network Pin Assignment information for the DDS interface cable.

Table 48 DDS Interface Cable Part Number

Cable and Interface Type	Part Number
DDS	9360119

Table 49 Network Pinout Assignments

PIN	SIGNAL
1	Transmit Ring
2	Transmit Tip
3	Not Used
4	Not Used
5	Not Used
6	Not Used
7	Receive Tip
8	Receive Ring

WPIM-E1

This section provides the Cabletron Systems part number and connector specifications for the WPIM-E1 interface cable.

Table 50 shows the WPIM-E1 connector number, cable and interface type, connector type and part number information.

Table 50 WPIM-E1 Connector Information

Connector Number	Cable and Interface Type	Connector Type	Part Number
1	E1	RJ45	9372095
2			

Table 51 provides WPIM-E1 network interface cable pin assignments.

Table 51 Network Interface

Pin	Signal
1	Receive Ring
2	Receive Tip
3	Shield Ground
4	Transmit Ring
5	Transmit Tip
6	Shield Ground
7	Not Used
8	Not Used

Table 52 provides WPIM-E1 DTE interface cable pin assignments.

Table 52 DTE Interface

Pin	Signal
1	Receive Ring
2	Receive Tip
3	Shield Ground
4	Transmit Ring
5	Transmit Tip
6	Shield Ground
7	Not Used
8	Not Used

Table 53 provides WPIM-E1 RJ45 network interface cable pin assignments.

Table 53 Network Interface

Pin	Signal
1	Receive Ring
2	Receive Tip
3	Not Used
4	Transmit Ring
5	Transmit Tip
6	Not Used
7	Not Used
8	Not Used

WPIM-DI

This section provides Cabletron Systems part number and connector specifications for the WPIM-DI interface cables.

Table 54 shows the connector number, cable assembly description, cable and interface type, connector type and part number information for the WPIM-DI interface.

Table 54 WPIM-DI Connector Information

Connector Number	Cable Assembly Description	Cable and Interface Type	Connector Type	Part Number
1	Network	DI	RJ48	9372094
2	Drop and Insert			

Table 55 provides the WPIM-DI network interface cable pin assignments.

Table 55 WPIM-DI Network

Pin	Signal
1	Receive Ring
2	Receive Tip
3	AC Coupled Ground
4	Transmit Ring
5	Transmit Tip
6	AC Coupled Ground
7	AC Coupled Ground
8	AC Coupled Ground

Table 56 provides the WPIM-DI drop and insert interface cable pin assignments.

Table 56 WPIM-DI Drop and Insert

Pin	Signal
1	Transmit Ring
2	Transmit Tip
3	AC Coupled Ground
4	Receive Ring
5	Receive Tip
6	AC Coupled Ground
7	AC Coupled Ground
8	AC Coupled Ground

WPIM-HDSL

This section provides connector specifications for the WPIM-HDSL interface cables. **Table 57** provides pin assignments for the RJ-45 network interface connector.

Table 57 WPIM-HDSL Network Interface Cable Pin Assignments

Pin	Signal
1	HDSL Loop 1 (Ring1)
2	HDSL Loop 1 (Tip1)
3	Not Used
4	HDSL Loop 2 (Ring2)
5	HDSL Loop 2 (Tip2)
6	Not Used
7	Not Used
8	Chassis Ground

WPIM-S/T

This section provides connector specifications for the WPIM-S/T interface cable. **Table 58** provides pin assignments for the RJ-45 network interface connector.

Table 58 WPIM-S/T Network Interface Cable Pin Assignments

Pin	Signal
1	Not Used
2	Not Used
3	Transmit +
4	Receive +
5	Receive -
6	Transmit -
7	Not Used
8	Not Used

C

Specifications and Standards Compliance

This chapter contains hardware specifications, and safety and compliance standards for the CSX400, CSX400-DC, and for the individual WPIMs that can be configured with these devices.

CSX400, CSX400-DC, and WPIM Environmental Requirements

Table 59 Environmental Specifications

Operating Temperature	5° to 40°C (41° to 104°F)
Storage Temperature	-30° to 73°C (-22° to 164°F)
Operating Humidity	5% to 90% RH, non-condensing

CSX400 Specifications and Compliance Standards

Table 60 Hardware Specifications

WAN Interface	2 WPIM ports
LAN Interface	2 EPIM ports
Other Interfaces	AC Power Connector
Processor	Intel i960 66 Mhz
Width	17 inches (43.2 cm)
Height	1.75 inches (4.5 cm)
Depth	13.5 inches (34.3 cm)
Weight	5.67 lbs (2.58 kg)
Power Supply	Built-in power supply
Voltage	100–125 Vac ~ 1.0 A, 200–240 Vac ~ 0.5 A
Frequency	50/60 Hz
Power Consumption	100 Watts maximum

CSX400-DC Specifications and Compliance Standards

Table 61 Hardware Specifications

WAN Interface	2 WPIM ports
LAN Interface	2 EPIM ports
Other Interfaces	dc power terminal strip
Processor	Intel i960 66 Mhz
Width	17 in (43.2 cm)
Height	1.75 in (4.5 cm)
Depth	13.5 in (34.3 cm)
Weight	5.67 lb (2.58 kg)
Power Supply	Built-in power supply
Voltage	48/60 Vdc ~ 3.5 A
Power Consumption	100 Watts maximum
Heat Dissipation	341.2 Btu/hr

CSX400 and CSX400-DC Regulatory Compliance

Safety — This unit meets the safety requirements of UL 1950, CSA C22.2 No. 950 and EN 60950, IEC 950, and 73/23/EEC.

EMC — This unit meets the EMC requirements of FCC Part 15, EN 55022, EN 50082-1, 89/336/EEC, AS/NZS 3548, CSA C108.8, and VCCI V-3.

CSX400-DC Regulatory Compliance (Only)

NEBS — This unit meets a minimum of Level 1 NEBS requirements in accordance with Bellcore SR-3580.

Individual WPIM Regulatory Compliance

The following sections provide regulatory compliance standards for the WPIM-TI, WPIM-SY, WPIM-DDS, WPIM-E1, WPIM-DI, WPIM-S/T, and the WPIM-HDSL. Cabletron Systems reserves the right to change these specifications at any time without notice.

WPIM-TI

This section describes the environmental specifications and safety and approval requirements for the WPIM-T1.

Safety — This unit meets the safety requirements of UL 1950, and CSA C22.2 No. 950.

Electromagnetic Compatibility (EMC) — This unit meets the EMC requirements of FCC Part 15, VCCI V-3, and CSA108.8.

NEBS — This unit meets a minimum of Level 1 NEBS requirements in accordance with Bellcore SR 3580.

TELECOM — FCC Part 68, CS-03.

WPIM-SY

This section describes the environmental specifications and safety and approval requirements for the WPIM-SY.

Safety — This unit meets the safety requirements of UL1950, CSA C22.2 No. 950, EN 60950, IEC 950, and 73/23/EEC.

EMI — This unit meets the EMI requirements of FCC Part 15, EN 55022, EN 50082-1, AS/NZS 3548, 89/336/EEC, CSA108.8, and VCCI V-3.

TELECOM — 91/263/EEC, and NET 2.

WPIM-DDS

This section describes the environmental specifications and safety and approval requirements for the WPIM-DDS.

Safety — This unit meets the safety requirements of UL1950, and CSA C22.2 No. 950.

(EMC) — This unit meets the EMC requirements of FCC Part 15, CSA108.8, and VCCI V-3.

NEBS — This unit meets a minimum of Level 1 NEBS requirements in accordance with Bellcore SR 3580.

TELECOM — FCC Part 68, CS-03.

WPIM-E1

This section describes the environmental specifications and safety and approval requirements for the WPIM-E1.

Safety — This unit meets the safety requirements of EN 60950, IEC 950, 73/23/EEC and AS/NZS 3260.

Electromagnetic Compatibility (EMC) — This unit meets the EMI requirements of EN 55022, EN 50082-1, AS/NZS 3548, and 89/336/EEC.

TELECOM — 91/263/EEC, CTR 12, TS 001, and TS 016.

WPIM-DI

This section describes the environmental specifications and safety and approval requirements for the WPIM-DI.

Safety — This unit meets the safety requirements of UL1950, and CSA C22.2 No. 950.

Electromagnetic Compatibility (EMC) — This unit meets the EMI requirements of FCC Part 15, VCCI V-3, and CSA108.8.

TELECOM — The WPIM-DI meets FCC Part 68 and CS-03.

WPIM-S/T

This section describes the environmental specifications and safety and approval requirements for the WPIM-S/T.

Safety — This unit meets the safety requirements of UC1950, CSA 22.2 No. 950, EN 60950, IEC 950 73/23/EEC.

Electromagnetic Compatibility (EMC) — This unit meets the EMC requirements of FCC Part 15, EN 55022, VCCI V-3, CSA/08.8 EN 50082-1, AS/NZS 3548, 89/336/EEC.

Telcom (Future) — FCC part 68, CS-03.

WPIM-HDSL

This section describes the environmental specifications and safety and approval requirements for the WPIM-HDSL.

Safety — This unit meets the safety requirements of UC1950, CSA 22.2 No. 950, EN 60950, IEC 950 73/23/EEC.

Electromagnetic Compatibility (EMC) — This unit meets the EMC requirements of FCC Part 15, EN 55022, VCCI V-3, CSA/08.8 EN 50082-1, AS/NZS 3548, 89/336/EEC.

NEBS — This unit meets a minimum of Level 1 NEBS requirements in accordance with Bellcore GR 1089.

D

Network Information Worksheets

Table 62 CSX400

Configuration Section	Item	Setting
System Settings	Router Name	
	Message	
System Settings Dial Authentication Password	Dial Authentication Password/Secret	
System Settings ISDN Settings	ISDN SPID #1 ISDN SPID #2 ISDN Directory Number #1 ISDN Directory Number #2 ISDN Switch Type	
System Settings Ethernet IP Address	Ethernet IP Address and Subnet Mask	
System Settings Ethernet IPX Network #	Ethernet IPX Network Number	

Table 63 Remote Router

Configuration Section	Item	Setting
Remote Router Database Dial Settings	ISDN Phone #1 ISDN Phone #2 Disconnect Timer Value Maximum Links Minimum Links Threshold Bandwidth Direction	
Remote Router Database Security	Minimum Authentication Remote Router's Password/ Secret	
Remote Router Database Bridging	Bridging On/Off Spanning Tree On/Off	

Table 63 Remote Router (Continued)

Configuration Section	Item	Setting
Remote Router Database TCP/IP Route Addresses	Remote Network's IP Addresses, Subnet Masks, and Metrics Source WAN IP Address and Subnet Mask ^a Remote WAN IP Address and Subnet Mask ^b	
Remote Router Database IPX Routes	IPX Routes: Network Number, Hop Count and Ticks	
Remote Router Database IPX SAPs	SAPs: Server Name, Server Type, Network Number, Node Number and Sockets WAN Network Number	

a. Used only in PPP numbered mode of addressing

b. Used only in PPP numbered mode of addressing



Make one chart for each remote router in the remote router database.

Table 64 Bridging and Routing Controls

Configuration Section	Item	Setting
Bridging/ Routing	Default Remote Bridging Destination TCP/IP Routing On/Off Internet Firewall On/Off IPX Routing On/Off	



FCC Part 68 - User's Information For CSX400 and CSX400-DC

The following instructions are to ensure compliance with the Federal Communications Commission (FCC) Rules, Part 68:

1. All connections to the WPIM-T1, WPIM-DI and WPIM-DDS must be made using standard plugs and jacks.
 - a. The WPIM-S/T must only be connected to the network connected behind an FCC Part 68 registered channel service unit. Direct connection is not allowed.
2. Before connecting your unit, you must inform the local telephone company of the following information:

Table 65 WPIM-DI and WPIM-T1

Port ID	REN/SOC	FIC	USOC
WPIM-DI WPIM-T1	6.0N	04DU9-BN 04DU9-DN 04DU9-1KN 04DU9-1SN 04DU9-1ZN	RJ48C RJ48X

Table 66 WPIM-DDS (Only)

Port ID	REN/SOC	FIC	USOC
WPIM-DDS	6.0N	04DU5-56 04DU5-64	RJ48S

Table 67 WPIM-S/T (Only)

Port ID	REN/SOC	FIC	USOC
(BR) WPIM-ST	6.0P	N/A (XD)	N/A (XD)

3. If the unit appears to be malfunctioning, it should be disconnected from the telephone lines until you learn if your equipment or the telephone line is the source of the trouble. If your equipment needs repair, it should not be reconnected until it is repaired.
4. The CSU/DSU has been designed to prevent harm to the T1 and DDS network. If the telephone company finds that the equipment is exceeding tolerable parameters, the telephone company can temporarily disconnect service, although they will attempt to give advance notice if possible.
5. Under the FCC Rules, no customer is authorized to repair this equipment. This restriction applies regardless of whether the equipment is in or out of warranty.
6. If the telephone company alters their equipment in a manner that will affect use of this device, they must give you advance warning so as to give you the opportunity for uninterrupted service. You will be advised of your right to file a complaint with the FCC.
7. The attached Affidavit on the following page must be completed by the installer.
8. In the event of equipment malfunction, all repairs should be performed by our Company or an authorized agent. It is the responsibility of the users requiring service to report the need for service to our Company or to one of our authorized agents. Refer to the **Getting Help** section of **Chapter 1**, for more information on how to get service and support.

**AFFIDAVIT FOR THE CONNECTION OF CUSTOMER EQUIPMENT
TO 1.544 MBPS AND/OR SUBRATE DIGITAL SERVICES**

For the work to be performed in the certified territory of

Telco's name: _____

State of: _____

Country of: _____

I, _____, of _____
(Name of Authorized Representative) (Customer Name)

_____, _____
(Customer's Address) (Telephone Number)

being duly sworn, state:

I have responsibility for the operation and maintenance of the terminal equipment to be connected to _____ 1.544 Mbps and/or _____ Subrate digital services. The terminal equipment to be connected complies with Part 68 of the Commission's rules except for the encoded analog content and billing protection specifications. With respect to encoded analog content and billing protection:

- I attest that all operations associated with the establishment, maintenance and adjustment of the digital CPE with respect to encoded analog content and encoded billing information continuously complies with Part 68 of the FCC's Rules and Regulations.
- The digital CPE does not transmit digital signals containing encoded analog or billing information which is intended to be decoded within the telecommunications network.
- The encoded analog and billing protection is factory set and is not under the control of the customer.

FCC Part 68 - User's Information For CSX400 and CSX400-DC

I attest that the operator(s) maintainer(s) of the digital CPE responsible for the establishment, maintenance and adjustment of the encoded analog content and billing information has (have) been trained to perform these functions by successfully completing one of the following: Check appropriate one(s).

- a. A training course provided by the manufacturer/grantee of the equipment used to encode analog signals; or
- b. A training course provided by the customer or authorized representative, using training materials and instructions provided by the manufacturer/grantee of the equipment used to encode analog signals; or
- c. An independent training course (e.g. trade school or technical institution) recognized by the manufacturer/grantee of the equipment used to encode analog signals; or
- d. In lieu of the proceeding training requirements, the operator(s) maintainer(s) is (are) under the control of a supervisor trained in accordance with _____ above.

I agree to provide _____ with proper documentation
(Telco's Name)

to demonstrate compliance with the information as provided in the proceeding paragraph, if so requested.

_____ (Signature)

_____ (Title)

_____ (Date)

Subscribed and sworn to me this _____ day of _____, 19____.

(Notary Public)

My commission expires:

F

Glossary

10BASE-T — IEEE 802.3 standard for the use of Ethernet LAN technology over Unshielded Twisted Pair wiring, running at 10 Mbps.

ARP — Address Resolution Protocol. An Internet protocol used to bind an IP address to Ethernet/802.3 addresses.

ASCII — American Standard Code for Information Interchange. It is an 8-bit code for character representation.

AUI — Attachment Unit Interface. An IEEE 802.3 transceiver cable connecting the network device (such as a router) to the MAU (media access unit).

Bandwidth on Demand — Feature providing the capability of adjusting the bandwidth (opening or closing multiple B channels) when the load in traffic increases or decreases.

Bridge — A device that segments network traffic. A bridge maintains a list of each node on the segment and only traffic destined for a node on the adjacent segment is passed across the bridge. A bridge operates at Layer 2 of the OSI reference model.

Bearer (B) Channel — A full duplex ISDN BRI or PRI 64 Kbps channel used for sending user data.

BRI — Basic Rate Interface. The ISDN interface providing two 64 Kbps B channels for voice, data and video transmission and one 16 Kbps D channel for signaling and data transmission.

CHAP — Challenge Handshake Authentication Protocol. A security protocol supported under point-to-point protocol (PPP) used to prevent unauthorized access to devices and remote networks. Uses encryption of password, device names and random number generation.

DCE — Data Communications Equipment. Equipment used within a network to transfer data from source to destination such as modems.

D Channel — In ISDN, a full-duplex 16 Kbps channel used for link setup.

Data Compression — Techniques used to reduce the number of bits transferred across the communication links that represent the actual data bits. Compression is used to optimize use of WAN links and speed data transmission.

DHCP — Dynamic Host Configuration Protocol is a protocol for automatic TCP/IP configuration that provides static and dynamic address allocation and management.

Dial on Demand — Dial up WAN resources are accessed only when remote access is required and released as soon as the resource is no longer needed.

DTE — Data Terminating Equipment. DTE refers to equipment used in a network as the data source and/or destination, such as computers.

DTMF — Dual Tone Multi-Frequency. TOUCHTONE as opposed to Dial Pulse (DP).

DTR — Data Terminal Ready. RS232 signal used for indicating to the DCE the readiness to transmit and receive data.

EtherTalk — AppleTalk protocols running on Ethernet.

Filter — Feature to control the flow of data based on protocol or bridge information. Filters can be specific to allow data through or prevent transmission.

Firewall — A combination of techniques used to protect one network from unknown networks and users on the outside. Firewalls can filter or block traffic and act as a management and network security point where all traffic can be scrutinized.

Frame — A group of data generated by Data Link Layer operation.

HDSL — High bit rate Digital Subscriber Line. A technology to put two-way T1 on a normal unshielded, bridged (but not loaded) twisted pair without using repeaters.

IMUX (Inverse Multiplexing) — The process of splitting a single high-speed channel into multiple signals, transmitting the multiple signals over multiple facilities operating at a lower rate than the original signal, and then recombining the separately-transmitted portions into the original signal at the original rate.

In-Band Signaling — Transmission within the frequency range used for data transmission; i.e., results in use of bandwidth normally reserved for data.

IP — Internet protocol. A network layer protocol which allows a packet to traverse multiple networks on the way to its final destination.

IP Address — Internet address. A 32-bit address assigned to devices that participate in a network using TCP/IP. An IP address consists of four octets separated with periods defining network, optional subnet and host sections.

IPX (Internet Packet Exchange) — A proprietary Network layer protocol developed by Novell and used in NetWare networks.

ISDN — Integrated Services Digital Network. Digital transmission standard defining communication protocols permitting telephone networks to carry data, voice, fax and other streams.

Leased Line — A telecommunications line between two service points leased from a communications carrier for private use, usually incurring a monthly service rate.

LEDs (Light Emitting Diodes) — Type of indicator lights on the panel of a device.

Local Area Network (LAN) — A network connecting computers over a relatively small geographic area (usually within a single campus or building).

MAC Layer/Address — Media Access Control layer/address defined by the IEEE 802.3 specification which defines media access including framing and error detection. Part of the OSI reference model Data Link layer.

Metric — An algorithm used by routers to determine the best path for transmitting packets to a remote destination based on considerations such as time, delay, cost, etc.

Modem — Modulator/Demodulator. A device that converts digital signals to/from analog signals for transmission over analog communications lines.

Multi-Link Protocol — A protocol, defined in RFC 1717, that defines a way to perform inverse multiplexing on the TCP/IP point-to-point protocol (PPP); i.e., the ability to use multiple serial WAN channels for transferring one datastream. With MLP, a user can send and receive data over both B channels in an ISDN basic-rate interface connection

NAT — Network Address Translation uses a unique IP address for a WAN interface. This IP Address is negotiated through PPP or assigned statically by the Internet Service Provider (ISP). NAT reduces the number of unique IP addresses for all clients using a particular WAN interface to one.

NetWare — A Network Operating System developed by Novell, Inc. providing shared access to files and other network services.

Network Layer — Layer 3 of the OSI reference model that provides the protocol routing function.

Node — Refers to a termination point for communication links; entity that can access a network.

OSI — Open System Interconnection. An international standard developed by ITU (formally CCITT) and ISO (International Organization for Standardization) to facilitate data networking multi-vendor interoperability. The OSI Reference Model defines seven layers, each providing specific network functions.

Packet — A group of data that includes a header and usually user data for transmission through a network.

Ping (Packet Internet Groper) — An echo message, available within the TCP/IP protocol suite, sent to a remote node and returned; used to test the accessibility of the remote node.

PPP (Point-to-Point Protocol) — A Data Link layer protocol that provides asynchronous and synchronous connectivity between computer/network nodes. Includes standardization for security and compression negotiation.

Q.921 — ISDN Data Link layer specification for the user-to-network interface.

Q.931 — ISDN specification for call set-up and signaling on ISDN connections.

RFC — Request for Comment. Documentation describing Internet communications specifications (e.g., Telnet, TFTP). Often these RFCs are used to achieve multi-vendor interoperability during implementation.

RJ11 — Standard 4-wire connectors for telephone lines.

RJ45 — Standard 8-wire connectors used for ISDN lines and 10 BASE-T connections.

RIP (Routing Information Protocol) — Protocols used in IP and IPX for broadcasting open path information between routers to keep routing tables current.

Routing — A Network layer function that determines the path for transmitting packets through a network from source to destination.

RS-232 — EIA standard specifying the physical layer interface used to connect a device to communications media.

Serialization Frames — Frames sent out by servers under IPX to check whether illegal copies of NetWare are in use on the network.

Service Advertising Protocol — Protocol used in IPX for broadcasting information about services available on the network, such as file servers, CD-ROM drives and modem pools.

SNMP — Simple Network Management Protocol. A widely implemented Internet network management protocol that allows status monitoring, getting/setting of parameters for configuration and control of network devices, such as routers and bridges.

Split B Channels — Each 64 Kbps ISDN B-channel can be used individually for a separate data connection.

Spoofing — Spoofing is a technique used to remove poll and update service frames from WAN links while ensuring that the network continues to operate normally. Spoofing is employed to minimize dial-up line connection time.

Subnet Address — An extension of the Internet 32-bit addressing scheme that allows the separation of physical or logical networks within the single network number assigned to an organization. TCP/IP entities outside this organization have no knowledge of the internal “subnetting.”

Subnet Mask — A 32-bit internet protocol address mask used to identify a particular subnetwork.

TCP/IP — Transmission Control Protocol/Internet Protocol. Refers to a set of internetworking protocols developed by the U.S. Department of Defense that define a two level layered approach for interoperability. TCP provides a connection-oriented Transport layer ensuring end-to-end reliability in data transmission. IP provides for Network layer connectivity using connectionless datagrams.

Telco Cloud — The “cloud” of switched virtual connections over a Wide Area Network (WAN).

TELNET — Internet standard protocol for remote terminal emulation that allows a user to remotely log in to another device and appear as if directly connected.

TFTP — Trivial File Transfer Protocol. A simplified version of the File Transfer Protocol (FTP) allowing for file transfer between computers over a network.

Transparent Bridging — Bridging technique used in Ethernet networks that allows transfer of frames across intermediate nodes using tables associating end nodes with bridging addresses. Bridges are unknown to the end nodes.

UDP — User Datagram Protocol. A connectionless protocol used to pass packets across an internet network, requiring no handshaking between source and destination.

Watchdog Frames — Frames sent out by servers to clients, under IPX, to verify that clients are still logged on.

Wide Area Network — A communications network that is geographically dispersed thus requiring links provided by communications carriers.

Workstation — Computer or terminal used by the systems administration or user.

Index

Numerics

10BASE2

- grounding 53
- link length 53
- specifications 53

10BASE-F

- attenuation
 - multimode 51
 - single mode 52
- link length
 - multimode 52
 - single mode 53
- specifications 51

10BASE-T

- impedance 50
- insertion loss 50
- link length 50
- specifications 50

A

AT & T 5ESS switch parameters 27

Attenuation

- 10BASE-F
 - multimode 51
 - single mode 52
- 10BASE-T 51

B

Bootstrap Protocol Client 158

Bootstrap Protocol Server 158

BRI configurations 25

Bridge filtering 18

Bridge Setup

- bridge port pair administrative status 151
- port administrative status 150
- spanning tree protocol 149

Bridging 16

Bridging and routing 17

Broadcast 160

C

Cable requirements 49

CHAP 12

Coaxial cable - see 10BASE2

Configuring the Network Broadcast Type on a port 160

Configuring the UDP Broadcast Redirector 158

Crosstalk 50

CSX-COMP/ENCR installation 62

D

Daughter Board 8

DC Power Supply Connections 70

Default Gateway 137, 139

Default Interface 137, 140

Directory numbers 25

DMS-100 switch parameters 28

Domain Name Server 158

Dynamic Host Configuration Protocol (DHCP) 11

E

EMC 241, 242, 243

EMI 242, 243

Enabling Forwarding on a port
IP 157, 166

Enabling Proxy ARP on a port 159

Enabling Routing Services on a port
IP 157, 166

Enabling the RIP Routing Protocol on a port 160, 170

F

- Fiber optics - see 10BASE-F
- Firmware Data Compression 10
- Flash Download
 - bootprom 146, 147
 - runtime 147
- Flash EEPROMs 7

G

- Getting help 4
- Grounding
 - 10BASE2 53

H

- Hardware specs 239, 240
- Host IP Address 136, 139
- Host Name Server 158

I

- IEEE 802.1d bridging 17
- IEEE 802.3 Ethernet 8
- Impedance
 - 10BASE-T 50
- Insertion loss
 - 10BASE-T 50
- Inverse Multiplexing (IMUX) 10, 100
- IP
 - about IP routing 17
 - Configuring the Network Broadcast Type on a port 160
 - Configuring the UDP Broadcast Redirector 158
 - Enabling Forwarding on a port 157, 166
 - Enabling Proxy ARP on a port 159
 - Enabling Routing Services on a port 157
 - Enabling the RIP Routing Protocol on a port 160, 170
 - internet firewall 18
 - Secondary IPs 76
 - Selecting a port for configuration 156, 164

- IP/IPX QuickSET routing
 - configuration 107 to 110

IPX

- about IPX routing 17
- enabling forwarding on a port 166
- enabling RIP on a port 170
- enabling routing services on a port 166
- enabling SAP on a port 168
- QuickSET IPX configuration 100

ISDN 14

- arranging service 23
- BRI line configuration 24
- types of switches 24

K

- Keyboard conventions 129

L

- LAN support 7
- Link length
 - 10BASE2 53
 - 10BASE-F
 - multimode 52
 - single mode 53
 - 10BASE-T 50
- Local Management
 - exiting screens 130
 - navigating menu screens 133
 - selecting menu screen items 132
- Local Management Screen Fields
 - command fields 128
 - display fields 128
 - event message field 128
 - input fields 128
 - selection fields 128

M

Management Agent 126

MIB

description 178

tree hierarchy 179

MIB Navigator

exiting 177, 180

navigation commands 179

other commands 180

special commands 180

MIB support 19

N

National ISDN 1 26

NETBIOS

Datagram Server 158

Name Server 158

Network Address Translator (NAT) 11

Network information worksheets 223, 245

Network Management

local 126

remote 126

NT-1 parameters 26

P

PAP 12

Phone numbers 25

Phys Address 137

Point-to-Point Protocol (PPP) 12

PPP 8, 9

Propagation delay 50, 52

Proxy ARP 159

R

Rack Mounting

accessory kit 8

Remote Network Management 7

Remote router worksheet 245

RIP 160, 170

Router configuration 29

directory numbers 31

IPX network numbers 37

IPX routes 37

IPX routing 36

IPX SAPs 37

ISDN line information 31

names and passwords 47

network diagrams 32

network information 30

network information tables 38

node numbers 38

phone numbers 31

sample configuration 42

source and remote IP addresses 33

SPIDs 31

TCP/IP default route 33

TCP/IP route addresses 33

TCP/IP routing 32

Routing 17

S

- Safety Requirements 242
- Selecting a port for configuration
 - IP 156, 164
- SNMP 19
- SNMP Community Names
 - read-only 18, 78, 142
 - read-write 19, 78, 142
 - super-user 19, 78, 142
- SNMP Traps
 - enable traps 144
 - trap community name 143
 - trap destination 143
- Software and firmware upgrades 22
- SPIDs 25, 26
- Subnet Mask 137, 139
- Sunrpc (NIS) 158
- Switch support 14
- Switches
 - AT&T 5ESS w/custom software 24
 - DMS-100 24
 - French Delta (VN4) switches 24
 - KDD (Kokusai Denshin Denwa Co., Ltd.) 24
 - National ISDN 1 (NI-1) 24
 - NET3 (European ISDN) 24
 - NET3SW (European Swiss-variant) 24
 - NTT (Nippon Telegraph and Telephone) 24
- System Date 136, 138
- System Time 136, 138

T

- TACACS-Database Service 158
- T-connectors 53
- Telephone switch parameters 26
- Telnet 131
- Time 158
- Trivial File Transfer 158
- Troubleshooting 205
 - bridging 215
 - power 208
 - software 214
- TCP/IP routing 215

U

- UDP
 - Bootstrap Protocol Client 158
 - Bootstrap Protocol Server 158
 - Configuring the Broadcast Redirector 158
 - Domain Name Server 158
 - Host Name Server 158
 - NETBIOS Datagram Server 158
 - NETBIOS Name Server 158
 - port numbers and requested services 158
 - Sunrpc (NIS) 158
 - TACACS-Database Service 158
 - Time 158
 - Trivial File Transfer 158

W

- Wire size 25
- Worksheets (network info) 223, 245
- WPIMs
 - WPIM-DDS 91 to 95
 - WPIM-DI 85 to 87
 - WPIM-E1 83 to 85
 - WPIM-SYNC 88 to 90
 - WPIM-T1 83, 85, 88

POWER SUPPLY CORD

The mains cord used with this equipment must be a 2 conductor plus ground type with minimum 0.75 mm square conductors and must incorporate a standard IEC appliance coupler on one end and a mains plug on the other end which is suitable for the use and application of the product and that is approved for use in the country of application.

GERMAN:

Die Netzleitung, die mit diesem Geraet benuetzt wird, soll einen zwei Leiter mit Erdleiter haben, wobei die Leiter mindestens 0.75 mm sind, mit einer normalen IEC Geraetesteckdose an einem Ende und einem Geraetestecker am anderen Ende versehen sind, der fuer den Gebrauch und die Anwendung des Geraetes geeignet und der zum Benuetzen im Lande der Anwendung anerkannt ist.

SPANISH:

El cable principal de la red eléctrica utilizado con este equipo debe tener 2 conductores y 1 toma de tierra con un mínimo de 0.75 mm² cada uno y necesita tener un aparato de acoplamiento standard IEC en un extremo y un enchufe para el cable principal de la red eléctrica en el otro extremo, lo cual sea adecuado para el uso y aplicación del producto y lo cual sea aprobado para uso en el país de aplicación.

FRENCH:

Le cordon d'alimentation reliant cet appareil au secteur doit obligatoirement avoir deux fils conducteurs de 0.75 mm² minimum et un fil de terre. Il doit également être équipé du côté appareil d'une fiche agréée IEC et du côté secteur, d'une prise adaptée à l'usage du produit et aux normes du pays où l'appareil est utilisé.